Prudently Secure Information Theoretic LSB Steganography for Digital Grayscale Images

Khan Farhan Rafat
Riphah Institute of Systems Engineering (RISE)
Islamabad, Pakistan

***Abstract*—The endangerment of online data breaches calls for exploring new and enhancing existing sneaky ways of clandestine communication to tailor those to match the present and futuristic technological and environmental needs, to which malicious intruders wouldn't have an answer. Cryptography and Steganography are the two distinct techniques that, for long, have remained priority choices for hiding vital information from the unauthorized. But the visibility of the encrypted contents makes these vulnerable to attack. Also, the recent legislative protection agreed to law enforcement authorities in Australia to sneak into pre-shared cryptographic secret keys (PSKs) shall have a devastating impact on the privacy of the people. Hence, the need of the hour is to veil in the encrypted data underneath the cover of Steganography, whose sole intent is to hide the very existence of information. This research endeavor enhances one of the most famous images Steganography technique called the Least Significant Bit (LSB) Steganography, from the security and information-theoretic standpoint by taking a known-cover and known-message attack scenario. The explicit proclamation of this research endeavor is that the security of LSB Steganography lies in inducing uncertainty at the time of bit embedding process. The test results rendered by the proposed methodology confers on the non-detectability and imperceptibility of the confidential information along with its strong resistance against LSB Steganalysis techniques.**

***Keywords*—Clandestine communication; covert channel; hiding data in plain sight; inveil communication; LSB steganography**

I. Introduction

The world is undergoing and witnessing significant information technology shift from a paper-based environment to a green, paperless digitized environment [1]. This drifting digitized world is called the Internet of Things (IoT) that constitutes a multitude of technologies, such as vehicles, locomotives, traffic lights, cameras, televisions, satellites, sensors, therapeutic apparatus, the drones, and smartphones, just to name some [2]. Today's Hi-Tec technological gadgetry is not only enchanting but also inebriating. Accustomed to the Hi-Tec tools, people now carry these everywhere in their journey across the world. Round the clock networking, coupled with allied Cloud computing, enables them to remain in contact with their loved ones besides handling appointments of significance and doing business on the fly, simultaneously [3], [4]. This fact is apparent from Fig. 1, which expounds on the dependency and reliance of the people on their smart digital gadgetry.

The situation above, though, speaks high of the technological cum digital revolution, indeed poses a higher risk of people falling prey to the oblivious enemy who continuously is keeping them under surveillance to invade their privacy [5]. It is but only the unawareness as regards breaches through user's unconscious sharing of personal data on social media that Gartner, in its data security breach report stated "cyber vulnerability" as one of the three significant areas of concern for the year 2020 [6].

A. *Privacy*

The word "privacy" refers to the degree or extent up to which people willingly share their private information with others [7]. However, the digitized world of today finds it cumbersome to preserve user's privacy from some intentional malevolent intrusion that has further amplified to many folds because of cutting edge technology and the skills with which the opponents have augmented themselves [8]. The realization of one's privacy dates back to the history of human civilization but is often considered not as their legitimate right. That disregarded facet stemmed from the fact that what felt private in one region contrasts in another [9]. This discrepancy, to the European Court of Human Rights and some prominent scholars upholding the notion, is due to devoid of consensus on one prescribed agreement on the legal definition of privacy [10]. This implication of privacy tied to its relationship with self-respect, and an individual's autonomy and freedom find itself confronted each day with the illicit masqueraders in this fast progressive Hi-Tec information-sharing cyberspace [11].

Amongst several techniques of information security, the two foremost runners in keeping information confined only to the authorized include Cryptography and Steganography [12].

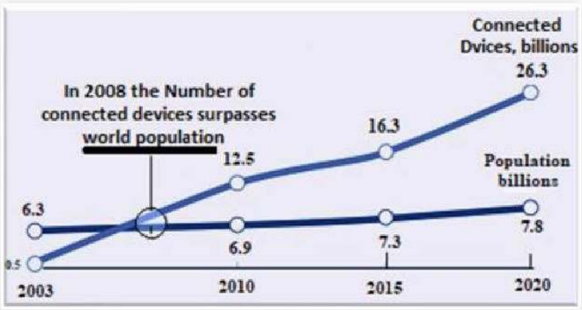


Fig. 1. Increasing Dependency and Reliance of the People on Smart Devices. Image Source [1].

B. *Cryptography*

The term Cryptography of Greek origin is a blend of two words: (i) crypto: meaning “hidden, secret”, and (ii) graphy: refers to' writing' respectively. It is more towards making the information unintelligible as regards its protection from unauthorized disclosure. The first acknowledged indication of its usage via some rarely used hieroglyphic symbols dates back to 1900 BC in an inscription imprinted in the tomb of Khnumhotep II, a nobleman of Egypt. The anticipation was not to hide the contents but to change the mannerism in which it appeared [13].

From the simplest Ceaser cipher [14] to Elliptic Curve Cryptography (ECC) [15], cryptography has undergone sophisticated computational advances because the techniques used in World War I and World War II have now become a matter of seconds to break on a personal computer by the hobbyist [16]. Today, cryptography has found its way in almost every field of life, including e-commerce, credit cards, digital cryptocurrencies, and Government and Corporate Sectors alike by transforming itself into an integral part of any information security infrastructure [13].

The originator of an encrypted entity shares with the intended recipients in prior, the decryption technique, and the encryption keys to impede compromise. As a convention, literature often uses the names Alice for the originator (abbreviated as 'A'), Bob (shortened to 'B') for the intended addressee, and Eve (' E' - the eavesdropper or 'W' - Warden Wendy) for the potential adversary [17]. Fig. 2 explains the encryption and decryption process, along with the terminology used.

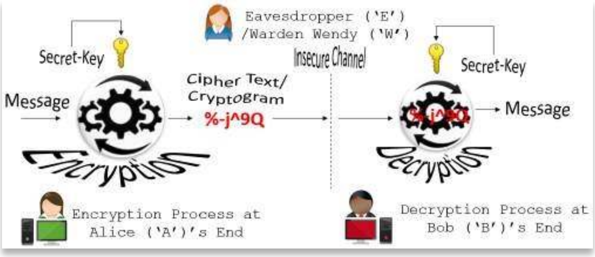


Fig. 2. Cryptographic System with allied Terminology.

1) Advantages: Some of the essential information security services that cryptography provides include:

- Confidentiality - Substituting message contents with arbitrary characters under the control of a shared secret called “secret/cryptographic key”, fades out the true context, thereby making it gibberish for an impostor/intruder.
- Authentication and Non-Repudiation - Digital signatures, using the Public-Private key-pair, protects against and counterfeits any spoofing attack.

2) Limitations: Following are some of the constraints that cryptography fell short of addressing:

- It fails to ensure the availability of information as and when required.
- It does not guarantee the veracity of the information.
- It cannot defend against weaknesses, which are a direct consequence of design flaws, whether that of system, processes, or protocols.
- It requires resources both in terms of computational time and power and money (infrastructure support).

a) Attacks on Cryptography: A variety of attacks [17–20] discussed below exists, whose very intent is to extract the meaning out of the encrypted contents without the knowledge of the secretly shared cryptographic key.

- Known Plaintext Attack - Knowing the plaintext for some portions of the ciphertext, the attacker tries to decrypt the remainder of the ciphertext via formulating some relationship between the two akin to determining the shared key.
- Chosen Plaintext Attack - Here, the attacker gets the plaintext of his/her choice encrypted. Using this plain-ciphertext pair make things easier in deriving the key used in encrypting the plaintext.
- Ciphertext Only Attack - Without having the corresponding plain contents, the attacker has access to a set of ciphertexts. The attack is a success if the conforming plaintext gets determined from those ciphertexts. This type of attack facilitates in deriving the encryption key, and hence any cryptosystem must guard against it.
- Brute Force Attack [21] - Knowing the keyspace, the attacker tries every possible combination to find out the key used for encrypting the plaintext. For example, given a key-size of 8-bits, the attacker applies all the possible 256 8-bit patterns (that is, 2^8=256) to decrypt the ciphertext. The attack, however, is resource-intensive, where the attacker might succeed in the very first attempt or continues until the last bit pattern.
- Dictionary Attack [22] - The attacker constructs a dictionary of ciphertexts along with corresponding plaintexts. Later, whenever a ciphertext needs to be analyzed, the same is searched in the dictionary in an attempt to retrieve the plaintext with subsequent dictionary updates.

b) Steganography: The name Steganography is an amalgamation of the two Greek words (i) steganos, which means “covered”, and (ii) graphy: which refers to “writing”. The name itself comes from Latin - Steganographia. Unlike cryptography, Its practical usage dates back to 440 BC [23]. It intends to hide the information traces as if those do not exist at all. Over some time, this technique has also evolved - from old unconventional methods ranging from shaving of the head and writing a message on the scalp, hiding message by engraving it on a lamb's belly to more recent microdot, invisible ink, null cipher, drifting from spatial to the frequency domain and hiding of data in multimedia files [24]. Fig. 3 gives the terminology and the process of secret message embedding and extraction [25].

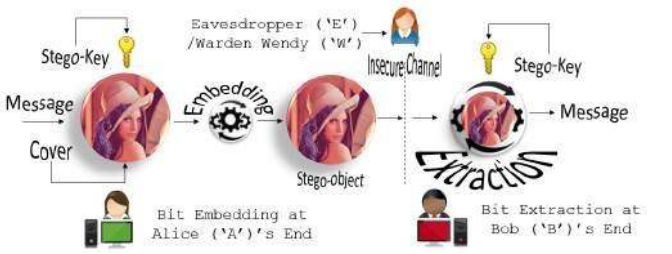


Fig. 3. The Steganography System with allied Lexicon.

3) Advantages: Following are some of the pros of the technique:

- Hides the existence of information as if that does not exist at all.
- With effective embedding methodology, the similarity between the cover and the Stego image makes detection of the embedded bits trivial because it shows some resembles for Gaussian noise.
- protects the anonymity of its recipients to some extent.

4) Limitations: Some of the cons of the technique include:

- The original cover used as a data carrier, ought to remain secret.
- The embedding algorithm losses its effectiveness if used without a Stego key.
- Security of Steganography System is often found misleadingly attributed to encryption of secret message bits before its embedding inside the cover.

a) The Gauging Parameters: The criteria to judge the effectiveness of a Steganography System include the triad of security, capacity, and imperceptibility [26], as shown in Fig. 4.

- Security - The Steganography System can withstand the traceability of the hidden information.
- Capacity - The maximum amount of information that the Steganography System can safely hide within the cover.
- Imperceptibility akin to undetectability - The ability of the Steganography System to at least minimize if not avoid the cover's degradation as regards secret information inset.

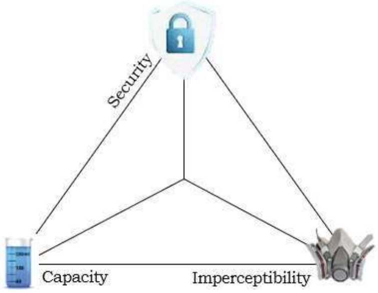


Fig. 4. Criteria to Gauge the Appropriateness of any Steganographic System.

It is, however, opined that imperceptibility is one of the components that ensure the security of the Steganographic System.

b) Attacks on Steganographic Systems: [27] has explained five types of aggression against any Steganographic system, and hence, it is but imperative for data hiding schemes to guard against those.

- Chosen Message attack - By selecting messages of choice, the attacker tries to examine the effects on the Stego-object to establish some relationship between the two.
- Known-Message attack - With the original message in hand, an attacker contrasts it with the generated Stego-object to patronize the bits for possible signatures for futuristic usage.
- Stego-Only attack - With only the Stego-objects in the possession and with the known algorithm, the attacker studies them to demystify the embedding.
- Known-Cover attack - Having the original cover alongside its corresponding Stego-object, the task of an attacker reduces to finding the differences between these two and extracting the hidden information.
- Chosen Stego attack - With selected Stego-objects, the attacker, works in conjunction with the algorithm to detect the embedded information.

This work is an extended version of the preliminary research carried out under the title "Nondeterministic Secure LSB Steganography for Digital Images", registered for presentation and publication in the international conference on Cyber Warfare and Security (ICCWS 2020), Pakistan.

The structuring of this endeavor is as follows: Section II discusses the basics of a digital image, it's processing, related domains, and the concept of bit-plane slicing, which is followed by a review of some recent LSB based Steganography schemes and its variant research in Section III. Section IV explains the research gap to address, which is derived from the literature review. Modeling considerations for our proposed method are discussed in Section V whereas LSB embedding and subsequent extraction methodology are the topics of Section VI. The details on the State-of-the-art in digital Image analysis and Steganalysis are showcased in Section VII. Section VIII explicates on the test results and their contrast with those of antecedents. Discussion on the contemporary and context-based issues under current pretext appears in Section IX. Section X concludes the proceedings.

II. Digital Image Steganography

A. Digital Image

A digital image composed of picture elements alias pixels has a finite, discrete numeric representation. That representation corresponds to image intensity called gray level at a specific place, which is the direct outcome of its two-dimensional spatial coordinates denoted with 'x' on the x-axis, and 'y' on the y-axis, respectively. Based on its modes of derivation or acquisition, such as placement of bits in a 2D format or scanning, a digital image may have the categorization of either a vector or raster type, respectively. The pixels reside as a raster image or raster map in a computer's memory, visualized as a two-dimensional array of integer values [28-29].

B. *Digital Image Processing*

Digital Image Processing (shortened as DIP) refers to pixels manipulating and transformation techniques that either enhances image quality such as noise reduction smoothing edges, or extracts information like features, with computerized algorithms.

C. *Bit Plane Slicing*

Set of bits that correspond to a specific bit position in each of the binary sequence representing the pixel value/intensity. For example, for 8-bit data representation (byte), there are 8-bit planes: the first-bit plane, while traversing from left to right, comprises the most significant bit (MSB), whereas the last that is, 8th position, contains the least significant bit (LSB). Fig. 5 gives the pictorial illustration of the concept.

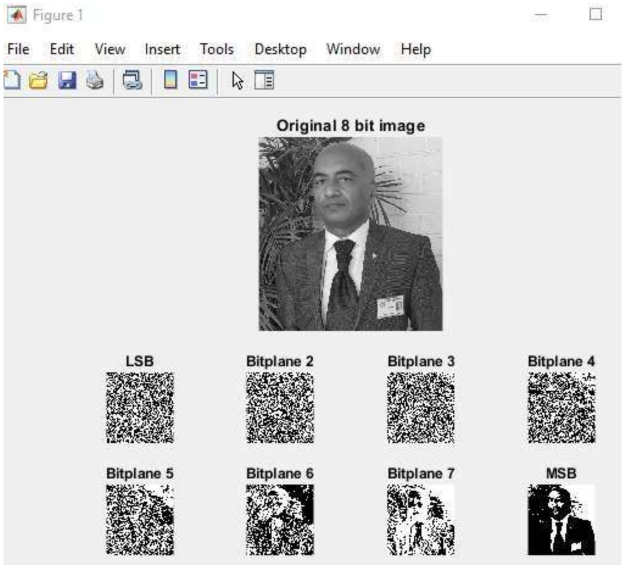


Fig. 5. Bit-Plane Slicing Illustrated.

As apparent from the figure above, the LSB plane contains information that does not profoundly contribute to image composition, whereas the MSB plane significantly contributes towards image visualization. The said characteristic of bit-plane slicing serves the basis for LSB Steganography.

D. *Domains of Image Processing: Most often discussed Image Processing Domains Include*

- Spatial Domain - In a 2D image representation (that in a matrix form), each element represents corresponding pixel intensity. This intensity distribution state of 2D matrices is called Spatial Domain. Recommended for working on images of real objects, some of the Steganography techniques related to this domain are the Modulus function, Pixel Value Differencing (PVD) [30], Least Significant Bit (LSB) (the focus of our proposed research), and Combination of LSB and PVD.
- Frequency Domain - A space where an image value at point P represents the amount that the image intensity values vary over an exact distance concerning P; that is, it gives the rate of change of pixel values. Preferred for working on images of modeled contours, some of the Steganography techniques of this domain include transformation methods such as Discrete Cosine Transform (DCT) [31] and Discrete Fourier Transform (DFT) [32].

E. *LSB Steganography*

Let $p[i]$ = {0, 1, . . ., 2^n-1} represent an n (=8) bit integer sequence where $p[i]$ denotes the pixel intensity of the i^{th} pixel in an 8-bit grayscale image. Hence, each $p[i]$ can then have a big-endian bit representation in terms of $b[i; 1]$; $b[i; 2]$; ... ; $b[i; n]$ for n number of bits using Eq. 1:

$$p[i] \leftarrow \sum_{k=1}^{n} b[i,k] * 2^{(n-k)} \quad (1)$$

LSB Steganography, as the name implies, operates by replacing the LSBs of each $p[i]$ with each message bit denoted by $msg[i]$, thereby rendering the Stego image as $stegO$[i]. The insertion of message bits is sequential and consecutive for each pixel comprising the cover image. The embedding process for the LSB insertion takes the form, per n pixels for distinct k, where k = 1. . . n, as shown in Eq. 2.

$$stegO\ (p[i]) = p[i, b_{lsb}] \leftarrow msg[w_{(j,l)}, b_k] \quad (2)$$

The w (j, l) is the corresponding l^{th} character of the word constituting the message, where j = {1,..., total words in the message}, l = {1, . . ., number of characters in the j^{th} word}, and b_k represents the distinct character bits.

III. Review of the Literature

One of the earliest accounts on digital Steganography goes to Kurak and McHugh [33]. The methodology proposed by them while examining image downgrading and contamination bear some resemblance to today's 4-bit LSBs (least significant bits) embedding. The author in [34] used a linear feedback shift register (LFSR) to generate pseudorandom numbers within a specified given range to locate the exact pixels for embedding bits of the secret data using the LSB technique. Arguably the assertion is that random pixel selection shall brace the security of LSB technique. The author in [35] first came up with an improved one-dimensional (1D) chaotic map by eliminating the inherent drawbacks of its narrower range of chaotic behaviors, and the uniform distribution of the key sequence. It followed the proposal of a color image LSB Steganography using their upgraded 1D chaotic map, which conferred on the exactness of the proposed bit embedding method. The author in [36] introduced an Optical Character Recognition (OCR) based Steganographic technique in which the feature form of the message got embedded in the target cover image. Extracted character-level features contained were embedded in the cover image to strengthening the data hiding because an impostor shall first know the hidden features, and even after that has to have a qualified OCR model to recover from the decoded contents (features). The results were found confirmatory to an English Printed Character dataset (Chars74K Dataset) for mixt LSBs. The author in [15] used the Elliptic Curve Cryptography (ECC) algorithm to encrypt the secret message and, after that, interleaved it into the cover by employing the LSB Inversion procedure. The author in [37] encrypted secret message before embedding it within LSBs of random multiple color pixels of the cover image using the Stern-Brocot Sequence. The author in [38] proposed a new technique using integer wavelet transform (IWT) to conceal patients' information by applying modified least significant bit (m-LSB) method to embed that into the randomly selected transform coefficients of an ECG signal via chaotic maps. The author in [39] doubly- layered reversible information hiding (RIH) method using the least significant bit (LSB) matching technique to improve the bit embedding efficiency (EE) and to enhance its quality by restraining the falsification instigated on to the Stego-image. The author in [40] used the LSB Steganography technique to hide images (as secret information) within the image, followed by scrambling Arnold technique to ascent the cover image for added security. The author in [41] proposed a mixt of cryptography, Steganography, and digital watermarking, calling it "Next Gen". The encrypted patient's information got embedded in the cover image using the LSB Steganography technique, and for authentication digital watermarking was used. The author in [42] presented a novel way of modifying true-color image pixels to facilitate high message bit embedding with least distortion by modifying at least one bit per Red (R), Green (G), and Blue (B) pixel to a maximum of 7 bits/pixel. Any bit position starting from LSB to 7th bit of the byte can appear modifiable. Arbitrary pixels with random bits used for hiding purposes for added security. The author in [43] suggested replacing the familiar words of English literature constituting the message with the values (128–255) of ASCII codes to use 8-bits in place of 8n bits, and converting those into respective binaries. Respective corresponding ASCII values are used for translating words other than those specified into bits. After rotating the cover image by some angle derived from the MSB and LSB of the secret key, the secret bits embedded in a spiral form pixel by pixel that is, either following a clockwise direction or counterclockwise based on the angle of rotation within the RGB. The channel that is, R, G, or B having the highest value gets secret data bits embedded into it under control of a secret key for which its most significant bit (MSB) is XORed with the LSB of the channel having the highest value. The XORed results decide which channel to use for embedding purposes. The offering of randomness by the two-step embedding serves the basis for [44]. Here, in the first stage, the secret encrypted quantum image is embedded into another quantum watermark image. After that, the quantum watermarked modified image is embedded into a quantum cover image using the optimal LSB-based algorithm. in the recovery phase, a series of inverse operations applied to retrieve the secret quantum image can be reconstructed by; only the Stego image, and the key can extract the secret quantum image. The author in [45] used modular arithmetic to hide secret data by avoiding the delinquent of overlapping. In the first instance, the target data to embed undergoes an intermediary conversion via another numbering system. The digits thus converted are embedded through articulating the intensities of the cover image in a manner that facilitates its easy retrieval at the receiving end. In their effort to increase bit embedding capacity of LSB Steganography technique [46] took inverting cover pixels in place of replacing those. The method involves finding the maximum and minimum values of the data that needs protection. This step is followed by subtracting all the secret contents from the maximum value. The results follow a division, and the new values thus obtained are inserted into the cover image to get the Stego-object/image. The author in [47] shared initial findings regarding modified LSB Steganography. By using r - indiscernibility relations, the authors embedded the secret data in a cover image in a semi-random manner. However, the same is reconstructable deterministically by employing a mask used during embedding. Each Byte of a cover pixel that contains a fixed combination of exact indiscernible bits with the mask serves as a placeholder for LSB replacement. The author in [48] linked the LSB matching method with the image enlargement technique to extend the extents of the Stego image. Doing so ensures an appropriate spread of secret information inside the Stego-image. The author in [49] proposed n-right most bit replacement technique for image Steganography for 1 n 4. The method iterates by converting the n-right most bits of every pixel and n-bits of the secret data to respective discrete values. By translating the difference of the two values, followed by the replacement of the cover pixels, produces Stego-image. The author in [50] proposed an LSB based Steganography method to hide secret data in digital images in a pseudorandom fashion via three chaotic noise generators based on the skew tent chaotic map. The author in [51] suggests utilizing a bit reversal method based on 2 schemes for improving the quality of Stego-image. The suggested schemes employee rearrangement of least significant bits of some of the pixels of the cover image if they are in proximity with a specific pattern of a few bits of the secret pixels. The author in [52] presented a high capacity image Steganography technique by blending pixel differencing and swapping mechanisms by dividing the image into 3 × 3 pixel non-overlapped chunks. LSB substitution is then applied on for every pixel within that chunk, followed by the application of quotient value differencing (QVD) on the leftover six bits. Because the proposed methodology is prone to fall off boundary condition, hence, that particular chunk stands undone from the said hybrid embedding, giving way to 4-bit LSB replacement. The author in [53] performs XOR-*ing* of the LSB of the red (R) in the RGB channel with the secret key bit that is, XOR (R_i, K_j), which determines the subsequent hiding of message bit in either Green (G) or the Blue (B) channels of RGB. If the result of the XOR operation is 1, the secret message bit is inserted as the LSB of G-channel else the B-channel LSB is replaced with a secret message bit.

IV. Research Problem

As evident from the literature reviewed, the majority of the effort rests in increasing bit embedding capacity of the cover image or to increase the perceptibility of the Stego image akin to increasing the system's security from the perspective of visual attack. However, the exertion in detecting hidden bits under a known-cover and known-message attack scenario is significantly missing. Things get further worse when the above situation gets linked to Kerckhoff's principle [54], which states that the security of a system lies in its key when that system is in a public domain. Hence, with the known algorithm, the cover, and the Stego image, the task of Wendy (the aggressor) equates only to detect and extract the embedded bits. The example that follows and as illustrated in Fig. 6, clarifies on the assertion.

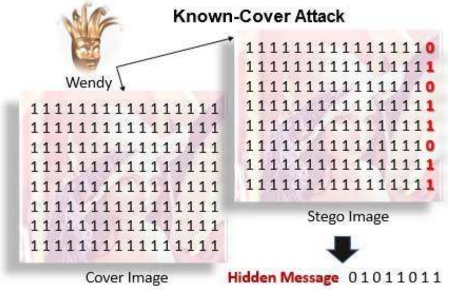


Fig. 6. Wendy Detects and Extracts the Hidden Message.

- Example: Let matrix A of order ($m \times n$) represent the cover image and let B denote the Stego image of the same order. Then the warden Wendy, in possession of the cover image and the known algorithm, needs only to contrast the two images to retrieve the hidden secret.

Using pseudo-random number generator (PRNG) to scatter bit embedding is illusionary, as [55] called the use of PRNG "a sin." It ought to mention here that most Steganography Systems prohibits the reusability of the cover, which is another pitfall of existing schemes.

Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR) seems overemphasized in recent studies in the context of Steganography as compared to the barely touched mean and standard deviation (STD) of an image. It is pertinent to mention here that PSNR is a measure of signal strength that does not take into consideration the human visual system (HVS) as compared to M/SSIM, which links HVS to illustrate the quality of an image.

In image processing, the “mean” accounts for the contribution of individual pixel's intensity towards the entire image, whereas standard deviation accounts for the dispersion of a pixel from mean that helps categorizes image regions.

V. Modeling the Proposed Steganography Algorithm

Simmons [56] proposed the first model for Steganography by taking a prisoner's problem whose elucidation is as follows:

- Alice and Bob were taken to prison, where they were locked up in separate cells. They were allowed to communicate with one another, but only through Warden Wendy, who on finding a clue of covert communication between the two, was authorized to send them in long imprisonment from where they could never return. Alice and Bob mutually shared some parameters for communication before they were taken into custody. The two must now agree on a scape plan using pre-agreed parameters.

Inspiration for our proposed model came from the fact that in addition to the limitations highlighted in Section IV, the pseudorandom number generation is also constraint by the fact that all the recipients engaged in communication must also have the same random number generator or that random sequence of numbers at their respective ends for appropriate bit extraction/message retrieval to succeed.

A facet of LSB insertion is that the inserted LSBs have a direct impact on the output statistics within the purview of the pixels/composition of the selected cover image. In our proposed algorithm, for example, the quality of the random number generator contributes significantly to the stego image quality. It is so because a True Random Number Generator (TRNG) produces different results each time of its use. It is this feature of TRNG that is, pure randomness, which information theory also supports [57] that explicitly points at the strength associated with its usage to achieve a secure information-theoretic solution as in our proposed solution. Additionally, the use of a TRNG, in our case, also eliminates the need for having it at recipient end for extracting hidden information, which is a compulsory requirement of techniques employing pseudo-random number generators. Doing above is advantageous to attain:

- an Information-Theoretic Secure Steganography Solution, and.
- reusability of the cover as opposed to the existing techniques where the original image is to be kept secret on its usage.

To achieve our set goal, we experimented with a MATLAB (*R2020a*)' *rand*' function for lateral replacement with a TRNG.

To facilitate ease and to speed up of the bit extraction and information retrieval process at the receiving end, we further favored (from futuristic requirements considerations as well) for a message header to keep the original message length (first six bytes of the header). It is followed by the file name, along with its associated content type (subsequent twelve bytes), that is, text, image, audio, video, and such other file types, which is followed by the actual message. The notation '*m*H' shall be used in the lateral discussion regarding any such message.

VI. Proposed Steganography Algorithm

The bit embedding and extraction processes are explicated as follows.

A. Bit Embedding Process

❖ Inputs:
i. Secret Message/Contents
ii. Cover Image
iii. Stego-Key (at least 4096 bits)
❖ Output:
i. Stego Image

To send a secret message, the initiator shall take the following steps:

1. Select a Stego-key of length ≥ 4096 bits.
2. Select the secret message/contents for embedding:
   a. by appending the message length (6 bytes), followed by content's filename (8 bytes) and type (4 bytes), that is, its extension.
   b. translating the whole text (*m*H) into its equivalent bits.

   c. translate Stego key into its equivalent bits.
   d. Exclusive-Or (XoR) mH with the Stego key bits. Extend the Stego key by replicating it till it equals mH length if needed.
3. Select the cover image.
4. Iterate through the cover image by taking one pixel at a time till the end of file (EOF).
   a. Replace the pixel's LSB with a random bit, preferably generated via a TRNG.
   b. Check the following:
      i. is the Stego key bit (moving from right to left) is ON?
      ii. is the pixel's MSB is OFF?
      iii. is the Stego key bit (moving from left to right) is ON?
      iv. are there still some secret message bits to process?
   c. If any of the answers above are FALSE then move to step (e).
   d. Replace the pixel's LSB with the secret message bit.
   e. If all the pixels are processed, then save the Stego image and move to step 5.
   f. Increment the message bit counter and decrement the Reverse counter.
   g. If the Reverse Counter reaches zero, reset it to the length of the Stego key.
5. Exit the bit embedding process.

The process above is illustrated in Fig. 7, and the corresponding source code is written in MATLAB as shown in Fig. 8.

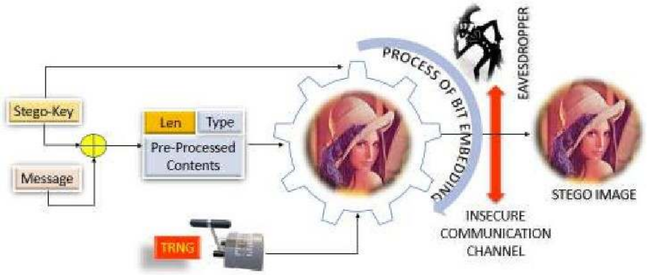
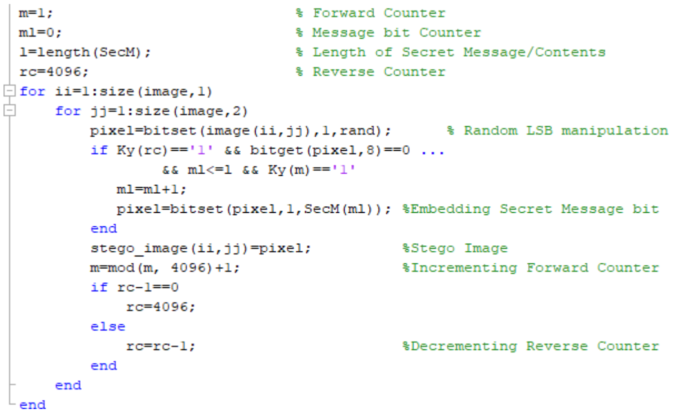


Fig. 7. LSB Substitution Illustrated.



```
m=1;                                % Forward Counter
ml=0;                               % Message bit Counter
l=length(SecM);                     % Length of Secret Message/Contents
rc=4096;                            % Reverse Counter
for ii=1:size(image,1)
    for jj=1:size(image,2)
        pixel=bitset(image(ii,jj),1,rand);      % Random LSB manipulation
        if Ky(rc)=='1' && bitget(pixel,8)==0 ...
                && ml<=l && Ky(m)=='1'
           ml=ml+1;
           pixel=bitset(pixel,1,SecM(ml)); %Embedding Secret Message bit
        end
        stego_image(ii,jj)=pixel;          %Stego Image
        m=mod(m, 4096)+1;                  %Incrementing Forward Counter
        if rc-1==0
            rc=4096;
        else
            rc=rc-1;                       %Decrementing Reverse Counter
        end
    end
end
```

Fig. 8. MATLAB Source Code for LSB Substitution in Grayscale Images.

B. Bit Extraction Process

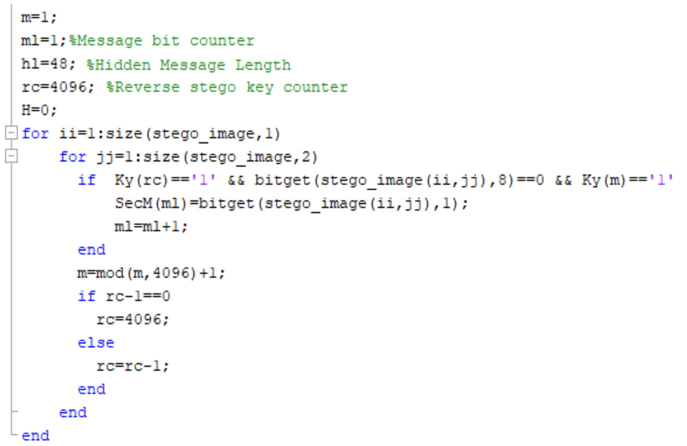
- ❖ Inputs:
  i. Stego Image
  ii. Stego-Key (Same, as used in embedding)
- ❖ Output:
  i. Hidden/Extracted Message

Following are the steps to extract the hidden message from the Stego image:

1. Select the pre-agreed Stego key and translate it into equivalent bits.
2. Select the Stego Image and iterate through it by taking one pixel at a time, first up to 144 bits to extract the hidden message length, file name along with its extension, and then up to the message length (just pulled) as per following procedure:
   a. Check the following:
      i. is the Stego key bit (moving from right to left) is OFF?
      ii. is the pixel's MSB is OFF?
      iii. is the Stego key bit (moving from left to right) is ON?
      iv. are 144 bits extracted? (or are there still some secret message bits to process?)
   b. If any of the answers above are FALSE, then move to step (e).
   c. Extract and store the pixel's LSB.
   d. If the extracted bits equal 144 in length or all the bits extracted as per hidden message length then:
      i. Exclusive-Or (XoR) the extracted bits with the Stego key bits.
      ii. Translate the results into bytes (8-bit chunks).
      iii. Once gone through, save or discard the message as applicable.
      iv. Move to step 3.
   e. Increment the message bit counter and decrement the Reverse counter.
   f. If the Reverse Counter reaches zero, reset it to the length of the Stego key.
3. Exit the bit extraction process.

As evident in the procedure above, supplemented by the MATLAB code of Fig. 9 and the bit extraction process shown in Fig. 10; does not necessitate the same TRNG at the receiving end. Moreover, there is no need to have a TRNG at the receiver's end for unidirectional communication.

Example - The following exemplifies the bit embedding and extraction processes of our proposed Information-Theoretic Secure LSB Steganography solution for grayscale images.



```
m=1;
ml=1;%Message bit counter
hl=48; %Hidden Message Length
rc=4096; %Reverse stego key counter
H=0;
for ii=1:size(stego_image,1)
    for jj=1:size(stego_image,2)
      if  Ky(rc)=='1' && bitget(stego_image(ii,jj),8)==0 && Ky(m)=='1'
          SecM(ml)=bitget(stego_image(ii,jj),1);
          ml=ml+1;
      end
      m=mod(m,4096)+1;
      if rc-1==0
        rc=4096;
      else
        rc=rc-1;
      end
    end
end
```

Fig. 9. MATLAB Bit Extraction Source Code.

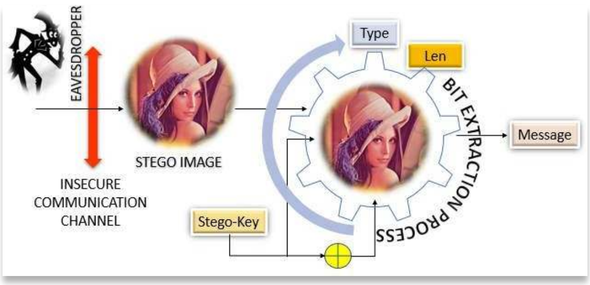


Fig. 10. Illustrating Bit Extraction Process.

Let:

i. S_k = 11001111 be the Stego Key bits

ii. *m*H = 00000110 denotes the secret message bits whose Exclusive-OR with the Stego key gives the result as mH ← 11001001 ← =XoR (11001111, 00000110)

iii. R_b = 1000010 be the randomly generated bits, and

iv. C_b = 00101000 01111010 represents the cross-section of pixels of the grayscale Cover Image.

1. Embedding Secret Message Bits - Step by step explanation is as follows:

   a. Pre-Processing of pixels

      i. Take the 1st pixel of the Cover Image that is, 10101000

      ii. Take the 1st random bit, that is, '1' and substitute it as the LSB in the selected Pixel as follows: 00101001 ← 00101000 ← 1

   b. Secret Message Bit embedding

      i. Because the MSB of the 1st cover pixel is 0, it is placed as the 1st pixel of the Stego image without secret message bit embedding.

      ii. The forward and reverse counters are incremented and decremented, respectively.

      iii. The 2nd cover pixel, that is, 01111010, is selected.

      iv. The pixel remains unaltered after pre-processing because the corresponding random and LSB bit is '0'.

      v. Because the 2nd most bits of the Stego key while traversing from left to right and right to left is ON (/1), and the MSB of the selected pixel is OFF (/0) as well, hence the 1st message bit that is, '1' is inserted as LSB of that pixel.

      vi. The processed pixel is then placed as the 2nd pixel of the Stego image.

   c. The Steps (a - b) above are repeated for all the pixels by continuous replacement of LSB bits with random bits meeting the aforesaid criteria, once all the secret message bits are processed. Thereafter, the Stego image is saved, and the bit embedding process terminates.

   d. The Stego image takes the form as 00101001 01111011 and is transmitted to the receiving end.

2. Bit Extraction Process - Step by step explanation is as follows:

   ❖ Given:

      i. Stego key S_k = 11001111

      ii. Pixels values (Stego Image) S_o = 00101001 01111011

   ❖ We need to find the hidden message = (*m*H) =?

   a. Extracting the Hidden Bits

      i. Because the MSB of the 1st cover pixel is 0, it is excluded from the bit extraction process.

      ii. By taking the 2nd pixel of the Stego image, it is observed that MSB of the pixel is OFF (/0). Also, the 2nd most bits of the Stego key while traversing from left to right and right to left is ON (/1) respectively, hence the LSB of that pixel, which is ON (/1), is extracted, and it is the first hidden encrypted message bit.

      iii. Exclusive-Or (XoR) the extracted bit with corresponding Stego key bit gives the hidden message bit. That is *m*H←0←XoR (1, 1).

      iv. Likewise, the above process continues until the extraction of all the secret message bits.

VII. Steganalysis Techniques and Image Quality Assessment Tools for Digital Image Steganography

The following elucidates on the state-of-the-art in image analysis that served as the foundation towards gauging the output as rendered by our proposed secure Steganography solution:

A. *Steganalysis*

The art and science of Steganalysis [58] aim at detecting and possibly extracting potentially veiled artifacts known as the payload (referred to as active Steganalysis [59]) from pragmatic data either with or without the prior knowledge of the underneath Steganography algorithm and allied parameters. This technique has gained significant prominence in forensic sciences and attained state-level recognition [60] in technically advanced countries [61] because detection or unveiling of the concealed information may help avoid and overcome catastrophic security situations. Recent interest in digital Steganalysis dates to the publication of the report regarding illegal usage of Steganography by the malevolent engaged in terrorist activities [62], which further got intensified after the 9/11 calamity [63-64].

1) LSB Steganalysis: With specific reference to the LSB Steganography technique, the LSB Steganalysis methods fall into three categories whose concise explanation follows subsequently and serves as a preferred choice in analyzing our proposed methodology:

a) Structural detectors [65] - Explicitly analyze the pairing structure of LSB substitution in pixel groups.

b) Weighted Stego-image (WS) [66-67] – Strives to estimate the embedded bits.

c) Statistical Detectors [68-69] – It is the application of analytical techniques to the embattled image.

The author in [70] presented a Least Significant Bits Steganalysis technique capable of detecting the existence of randomly scattered hidden data embedded in the LSBs of natural continuous-tone images. The method precisely measures the embedded message length, even for lengths that are relative to the target image size. It works by forming some subsets of pixels whose cardinalities vary with LSB embedding, and which can precisely be quantified.

The author in [67] enhances the Weighted Stego-Image (WS) Steganalysis method evolved for LSB replacement payload size estimation in digital images. In doing that, the study suggested for up-gradation of the three components, namely bias correction, the cover pixel prediction, and the least-squares weighting. Experimental results spread over more than two million attacks in total, which were based on images from numerous sources, and pre-processing antiquities showed significant improvement in the accuracy leaving behind the best of the structural detectors by avoiding their high rate complexity.

In contrast to the Least Significant Bit (LSB) Steganography, Steganalysis uses structural or combinatorial traits of the LSB embedding. The author in [65] suggested a general framework for detecting hidden messages along with giving an estimate of their length by including all the combinatorial structures covering those of the earlier research. Experimental evidence suggested a higher success rate of detection for the proposed method in contrast to that of its competitors.

The author in [71] suggested the detection of hidden messages in the Least Significant Bit (LSB) plane of an original image under the assumption that the mean level and the covariance matrix of that image are unknown. The adaptive statistical test was so designed that the anticipated distribution shall remain independent of the parameters of the referral image, and yet ensuring the highest probable degree of detection of the hidden bits. The test replaces the estimates developed on a local linear regression model with those of the unknown parameters. It was shown that the probability of detection gets maximized with the increased image size, which served as an asymptotic upper bound for the detection of hidden informative bits.

2) Image Quality Assessment (IQA): With the abundance of varied digital multimedia contents like audio, video, and such other file formats for data concealment [72-73], this research focuses on 8-bit grayscale digital images for its usage as a cover in carrying secret information and hence, shall only discuss the said technique from that facet. The justification in selecting digital images for our proposed secure Steganography solution is that being the most preferred media type after textual communication, these easily pass unnoticed through information barriers. This trait is because of their success in exploiting the human visual system (HVS) [74–77], contrary to the text where a single bit change results in an erroneous character. Further, their layout provides several redundant and partisan areas such as edges that serve as regions of interest (ROI) [77–79] for embedding information, which most of the contributions on the subject [80–82] have exploited for increased payload.

However, the insertion of information bits within a digital cover is likely to affect the cover's quality [83], which tends to make it a subjective matter [84]. It is because the perception of quality varies from person to person, and hence, it is unlikely to have an unbiased agreement on that matter. The situation above calls for having an Image Quality Assessment (IQA) methods/metric to quantify the image's quality objectively for reference [85], and which shall remain globally acceptable.

Since the approaches adopted for digital image analysis considers either a change in features between the original image/cover and the modified image called a visual attack or rely on the statistics of the modified image contents, including its type, expected payload length and such other attributes, hence, in the purview of a reference image, the IQA methods fall into three categories as follows:

a) Full Reference [86]: The method assumes to have an undistorted original reference image for comparison with an altered image, and hence destined to maintain accuracy in terms of the results. In the context of Steganography, this method is analogous to the most lethal known cover attack, which is the prima face of our proposed research. Following serves as some of the performance measures:

1) Absolute Difference (AD) – It is an effective similarity measure that gives the absolute difference between the referenced and the filtered (altered) image by subtracting the corresponding elements of the two matrices, as shown in Eq. 3.

$$AD = \sum_{i=1}^{N} \sum_{j=1}^{M} |R\ (i,j) - T\ (i,j)| \qquad (3)$$

2) Maximum Difference (MD) – It quantifies an image's contrast level by using Eqn. 4 and ranges from 0 to any of the positive values. However, the higher the value, the more inferior the image's quality.

$$MD = max\,|R\ (i,j) - T\ (i,j)| \tag{4}$$

3) Mean Absolute Error (MAE) – Suitable to measure the blurring effect of an image with the ideal value being zero. Calculated using Eqn. 5, a higher value indicates a degraded quality image.

$$MAE = \frac{1}{(M \times N)} \sum_{i=1}^{N} \sum_{j=1}^{M} |R\ (i,j) - T\ (i,j)| \tag{5}$$

, where M × N is the size of the images, R (i, j), and T (i, j) are the referenced and tarnished image sequentially at the i^{th} and j^{th} location.

4) Mean Square Error (MSE) – As the name suggests, it computes the mean square difference between the referenced and distorted images by using the formula shown in Eq. 6. MSE is the image quality measure typically when used for noise detection or blur removal, and henceforth.

$$MSE = \frac{1}{(M \times N)} \sum_{i=1}^{N} \sum_{j=1}^{M} |[R\ (i,j) - T\ (i,j)]^2| \tag{6}$$

, where M × N is the size of the images that is, i =1, .., M; j = 1, . . . , N. The anticipated value for MSE ≥ 0, where zero is the ideal result.

5) Root Mean Square Error (RMSE) – It is the square root of mean squared error (MSE) computed via equation Eq. 7.

$$RMSE = \sqrt{}(\frac{1}{(M \times N)} \sum_{i=1}^{N} \sum_{j=1}^{M} |[R\ (i,j) - T\ (i,j)]^2|) \tag{7}$$

The range of RMSE is ≥ 0, where zero stands as the ideal value.

6) Peak Signal-to-Noise Ratio (PSNR) – It is a measure of the signal's strength and calculated using equation Eq. 8. For Steganography, it is being used as a quality measure though it is independent of the human visual system (HVS).

$$PSNR = 10\ log_{10} \frac{P^2}{MSE} \tag{8}$$

The ideal value for PSNR is ∞. However, values > 0 are acceptable, where P is the highest gray level in the image, and MSE is computed using Eq. 6.

7) Laplacian Mean Squared Error (LMSE) – It is a measure of image degradation on account of factors such as edges, noise, and such other effects and calculated as shown in Eq. 9. The larger the value of LMSE, the poor shall be the quality of the target image.

$$LMSE = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} |[O(R\ (i,j)) - O(T\ (i,j))]^2|}{\sum_{i=1}^{N} \sum_{j=1}^{M} |O(R\ (i,j))|^2} \tag{9}$$

, where O (R (i, j)) = R (i + 1; j) + R (i – 1, j) + R (i, j + 1) + R (i, j − 1) − 4×R (i, j).

8) Normalized Cross-Correlation (NCC) – It enhances the image brightness by the normalization process and is widely used for image restoration purposes. Computed by using Eqn. 10, the range of NCC varies between ±1, where a −1 indicates a perfect correlation, and +1 a negative correlation.

$$NCC = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} R\ (i,j) \times T\ (i,j)}{\sum_{i=1}^{N} \sum_{j=1}^{M} R\ (i,j)^2} \tag{10}$$

9) Cosine Similarity (CS) − It is computed by taking into consideration the cosine of the angle between two vectors in a multidimensional space. It is a measure of the similarity between the two vectors because the value of the measure increases with the decrease in the angle between them, and is calculated using equation Eq. 11.

$$CS = \frac{\sum_{i=1}^{N} R_i \times T_i}{\sum_{i=1}^{N} {R_i}^2 \times \sum_{i=1}^{N} {T_i}^2} \tag{11}$$

, where R_i and T_i are the components of vectors R and T respectively. The similarity equals 1 when both the R and the T are the same, or is -1 if the two are opposite. A value of zero for CM means no correlation.

10)Structural Content (SC) − The structural content is concerned with the spatial arrangements of the pixels in an image. It is a similarity measure between the two images human eye cannot differentiate and is computed by using Eq. 12.

$$SC = \frac{\sum_{i=1}^{M} \sum_{j=1}^{N} T(i,j)^2}{\sum_{i=1}^{M} \sum_{j=1}^{N} R(i,j)^2} \tag{12}$$

The best value of SC is 1.

11)Structure Similarity Index (SSIM) – It gives a comparison between the luminance as given in Eq. 13, contrast, as in Eq. 14, and that for the structure, as shown in Eq. 15 of the referenced and target images where the SSIM is computed, as shown in Eq. 16 and Eq. 17.

$$L(uminance)_{AB} = \frac{2\mu_A\mu_B + C_1}{{\mu_A}^2 + {\mu_B}^2 + C_1} \tag{13}$$

$$C(ontrast)_{AB} = \frac{2\sigma_A\sigma_B + C_2}{{\sigma_A}^2 + {\sigma_B}^2 + C_2} \tag{14}$$

$$S(tructure)_{AB} = \frac{\sigma_{AB} + C_3}{{\sigma_A}^2{\sigma_B}^2 + C_3} \tag{15}$$

$$SSIM_{AB} = {L_{AB}}^{\alpha}, {C_{AB}}^{\beta}, {S_{AB}}^{\gamma} \tag{16}$$

, with the weights α, β, and γ = 1, Eq. 16 takes the form, as shown in Eq. 17.

$$SSIM_{AB} = \frac{(2\mu_A\mu_B + C_1)(2\sigma_A\sigma_B + C_2)}{({\mu_A}^2 + {\mu_B}^2 + C_1)({\sigma_A}^2 + {\sigma_B}^2 + C_2)} \tag{17}$$

The values of α, β, and γ define the weight assigned to each model, μ_A, μ_B are the averages of signal A and B as in Eq. 18, C_1= $(K_1P)^2$, P is the highest gray level value in Eq. 19, C2= $(K_2P)2$, K_2≤1. C_3 = C_2/2, and σ_{AB} denotes the standard deviation between signals (A, B) as in Eq. 20.

$$\mu_A = \frac{1}{M} \sum_{i=1}^{M} A_i \tag{18}$$

$$\sigma_A = \sqrt{\frac{1}{M} \sum_{i=1}^{M} (A_i - \mu_A)\ ^2} \tag{19}$$

$$\sigma_{AB} = \frac{1}{M-1}\sum_{i=1}^{M}(A_i - \mu_A)(B_i - \mu_B) \quad (20)$$

b) Reduced-Reference (RR) − Proposed by [87], and also known as the partial reference (PR) method, predicts the quality of the target image where only certain aspects of the original image are known. Here, the sender, apart from sending the image over a noisy/insecure/narrow bandwidth channel, transmit along an auxiliary channel some of the extracted features that contribute towards the quality assessment of the reference image, doing this aimed at facilitating the correct /simple retrieval of the original image by the recipient. Depending on the methodology, the receiver may adjust a specific aspect of the altered/received image to reconstruct the same and expound on the quality in the context of the referenced image. Fig. 11 is an illustration of the said concept. However, the availability of an auxiliary channel is a prerequisite for the above method to work.

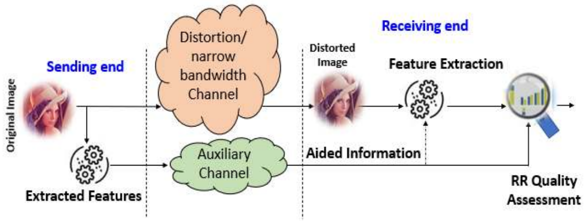


Fig. 11. Illustrating Reduced Reference Image Quality Assessment System.

c) No-Reference (NR) [88] − As the name suggests, the NR method akin to the blind image quality assessment (BIQA) method, does not require a reference image. Instead, the quality assessment is based on the features of the target image. This method parallels a real-time scenario where no reference image is available for cross-comparison and hence, must also be given due consideration.

1) Blind/Reference less Image Spatial Quality Evaluator (BRISQE) − [89] presented a blind/no-reference (NR) image quality assessment (IQA) model that works for the spatial domain. The model, blind image spatial quality evaluator (BRISQE), uses scene statistics of locally normalized luminance coefficients to enumerate probable losses of “genuineness” in the image due to the presence of misrepresentations, that leads to a holistic quality measure. The model does not need transformation to another domain, such as Discrete Cosine Transformation (DCT), Wavelet, and such other transformations. Statistical results show BRISQE superiority over full-reference peak signal-to-noise ratio (PSNR) and the structural similarity index (SIM).

2) Naturalness Image Quality Evaluator (NIQE) – It is an opinion-unaware, IQA method that uses Naturalness Image Quality Evaluator to calculate the no-reference image quality score for the input image. NIQE can ascertain the quality of a distorted image. Decreasing NIQE increases the perceptual quality of the image [90].

3) Perception-based Image Quality Evaluator (PIQE) − [91] proposed a novel no-reference IQ Evaluator real-world imagery. Unlike opinion-based supervised learning, an opinion-unaware methodology quantifies the distortion within an image without any training data but relies on pulling out local features for forecasting quality. Additionally, to mimic human behavior, we estimate quality only from perceptually significant spatial regions. Low computational complexity is another facet of the algorithm.

4) Singular Value Decomposition (SVD) − [92] presented a new grayscale image quality assessment measure to predict the distortion contributed by a variety of noise sources. Five test images, namely airplane, boat, Goldhill, Lena, and peppers with six types of alteration including JPEG, JPEG 2000, Gaussian blur, Gaussian noise, sharpening, and DC-shifting, each with a distortion level of five, were subjected to quality assessment via this method. The measure performed well when compared with PSNR and such other similar measures.

The SVD requires one input matrix and yields three matrices as output. Using a Matrix, A of size m × n the computation is performed as shown in Eq. (21),

$$S = SVD(X) \quad (21a)$$

$$[U, S, V] = SVD(X) \quad (21b)$$

$$[U, S, V] = SVD(X; 0) \quad (21c)$$

where U and V are the orthogonal matrices while S is a diagonal matrix. SVD computes the norm of the diagonal matrix S, which gives the correlation between the pixels in a specific matrix. The best matching occurs when the difference between the two norms equals zero. The authors in [93], [94] also explicate on blind image analysis. To implement the above in MATLAB programming language, [95] serves a good reference.

VIII. Evidence-based Test Results

A total of 30 grayscale images of dimension 512 × 512, as shown in Fig. 12, were selected from the dataset [96] and other freely available web resources for Steganalysis and tested against full, reduced, and no-reference models. All the cover images were in Tagged Image File Format (TIF/TIFF), where maximum sustainable randomly generated bits were used as a message.

A. Results for Steganalysis

The Steganalysis outcome and other statistics shown in Table I elucidates on non-detection of LSB insertion by [65–70] for the said images when processed through our proposed secure steganographic bit embedding algorithm, the theoretical aspects of which are covered in Sec. IX.

B. Full Reference Test Results

Full Reference validity conducted using the MSSIM, SC, MSE, LMSE, NAE, MAE, WPSNR, NCC, CS, and AD. Table II expounds on the output, which speaks high of our proposed secure bit embedding algorithm.

It is also pertinent to mention here that the cosine similarity (CS) for all the test images was found out to be one and hence, is not listed. The NCC of some of the test images is shown in Fig. 13 for visual illustration.

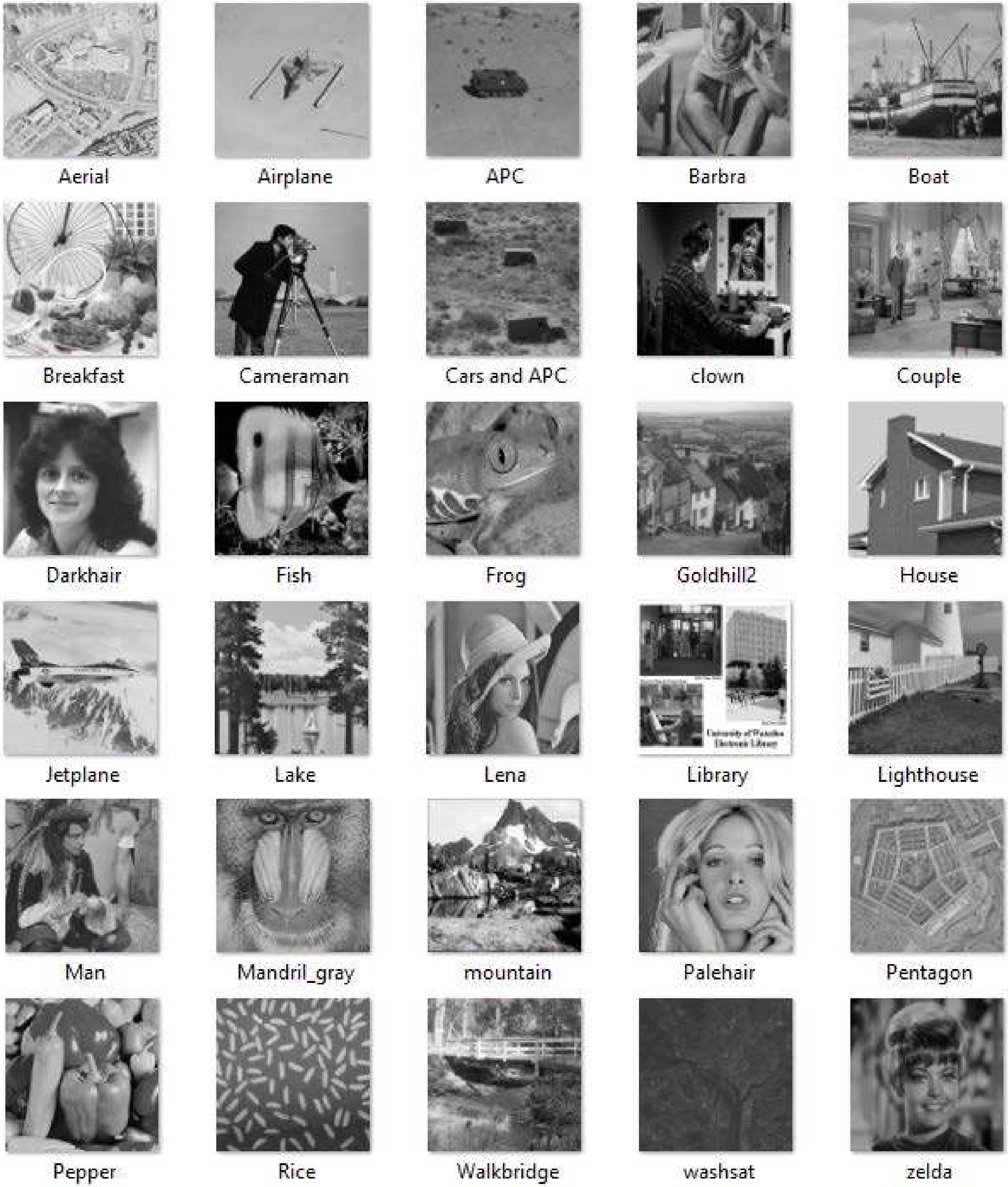


Fig. 12. 512 × 512 Grayscale Test Images [96].

TABLE I. SECURITY

Test Images	Maximum		Entropy				Steganalysis				
	M. Bits	bpp	R. Ent	S. Ent	MI	J. Ent	RS	SP	Triples	WS	AUMP
APC	17127	0.0654	5.0534	4.9338	4.7897	5.1976	0.1972	0.1046	0.0145	0.0783	3.152
Aerial	6108	0.0234	6.994	6.048	5.9971	7.0449	0.1187	0.0161	0.0013	-0.027	0.3923
Airplane	2412	0.0093	4.0045	3.9954	3.9751	4.0248	0.0048	-0.0109	0.0013	0.0012	0.2105
Barbra	37856	0.1445	7.4664	6.7877	6.4676	7.7865	0.2975	0.2064	0.3684	0.1269	4.1021
Boat	18672	0.0713	7.1238	6.2889	6.1322	7.2805	0.1258	0.0207	0.0175	0.0222	1.9404
Breakfast	14920	0.0570	7.5423	6.668	6.5434	7.6668	0.0888	-0.0696	0.0152	0.0161	5.9851
Cameraman	25622	0.0978	7.048	6.2691	6.0536	7.2634	0.1126	0.0892	0.0332	0.0661	9.0315
Cars and APC	44140	0.1685	6.5632	6.3966	6.0239	6.9359	0.3961	0.2096	0.3684	0.1861	3.576
Couple	32220	0.1230	7.2952	6.6634	6.3925	7.5661	0.2544	0.1388	0.3684	0.1029	4.1144
Darkhair	40408	0.1542	7.2767	6.6226	6.2823	7.617	0.2079	0.1143	0.0739	0.1429	14.0275
Fish	39801	0.1519	7.3988	6.7599	6.4236	7.7351	0.1808	0.1955	0.0658	0.1266	19.0433
Frog	35655	0.1361	7.0366	6.3404	6.0397	7.3372	0.3442	0.3047	0.3684	0.1863	3.5217
Goldhill2	43237	0.1650	7.4778	6.8427	6.4787	7.8418	0.2892	0.2054	0.3684	0.1217	4.7349
House	35878	0.1369	5.7529	5.2777	4.9738	6.0567	0.1067	0.051	0.0221	0.0887	15.9681
Jetplane	11545	0.0441	6.7135	5.8139	5.717	6.8104	0.0726	0.0437	0.0061	0.0121	1.7099
Lake	32667	0.1247	7.4826	6.7572	6.4846	7.7553	0.1576	0.0352	0.0226	0.0558	1.5588
Lena	31227	0.1192	7.4456	6.7083	6.4469	7.707	0.1372	0.2942	0.0325	0.0761	3.8846
Library	28315	0.1081	6.8562	6.2446	6.0066	7.0941	0.1016	0.06	0.0053	0.0341	2.12
Lighthouse	40906	0.1561	7.4486	6.8356	6.4905	7.7936	0.283	0.281	0.0627	0.1212	5.5697
Man	35528	0.1356	7.2367	6.5587	6.259	7.5365	0.254	0.1616	0.0611	0.1328	7.9212
Mandril gray	30728	0.1173	7.2925	6.5508	6.2933	7.55	0.3758	0.1408	0.0413	0.0893	4.869
Palehair	22802	0.0871	6.9542	6.3037	6.1122	7.1457	0.1467	0.2247	0.0279	0.0708	2.7151
Pentagon	19534	0.0746	6.6548	5.8213	5.6566	6.8195	0.2653	0.1268	0.0272	0.1005	3.2404
Pepper	33117	0.1264	6.7624	6.5306	6.2504	7.0427	0.1522	0.2028	0.0631	0.1234	7.6063
Rice	45744	0.1746	7.0171	6.4051	6.0196	7.4026	0.2398	0.1807	0.0633	0.1307	6.2447
Walkbridge	39859	0.1521	7.683	7.0288	6.6927	8.0191	0.3136	0.1452	0.0489	0.1138	3.5319
clown	49431	0.1886	5.3684	5.7861	5.3684	5.7861	0.2089	0.1414	0.0993	0.1702	14.5023
mountain	29538	0.1128	7.7828	7.0395	6.7919	8.0304	0.269	0.1813	0.0253	0.047	2.7038
washsat	62489	0.2384	2.8676	3.3938	2.8676	3.3938	0.2502	0.2348	0.1159	0.2001	12.4087
zelda	48486	0.1850	7.2668	6.6769	6.2676	7.6761	0.2666	0.2094	0.3684	0.1479	6.5424

bpp = Bits Per Pixel; R. Enrt = Entropy of Reference Image; S. Entr = Entropy of Stego Image;
J. Entr = Joint Entropy; MI = Mutual Information

TABLE II. FULL REFERECE (FR) IQA

	Maximum	Test Results								
File Name	M. Bits	MSE	RMSE	LMSE	NAE	MAE	PSNR	WPSNR	NCC	AD
APC	17127	0.2994	0.5472	0.008	0.0024	0.2994	53.3686	60.6857	0.0684	-0.2696
Aerial	6108	0.5024	0.7088	0.0028	0.0028	0.5024	51.1205	63.7239	-0.0105	-0.4907
Airplane	2412	0.4334	0.6583	0.0146	0.0025	0.4334	51.7619	62.6107	0.0700	-0.4285
Barbra	37856	0.5001	0.7072	0.0024	0.0044	0.5001	51.1405	57.3499	0.0052	-0.4271
Boat	18672	0.4907	0.7005	0.0088	0.0036	0.4907	51.2224	59.7254	0.1088	-0.4544
Breakfast	14920	0.4982	0.7058	0.0198	0.0029	0.4982	51.157	59.9982	0.0277	-0.4696
Cameraman	25622	0.5002	0.7072	0.0293	0.0042	0.5002	51.1392	60.2802	0.0955	-0.4515

Cars and APC	44140	0.4765	0.6903	0.0056	0.0045	0.4765	51.3502	60.4525	0.0097	-0.3946
Couple	32220	0.4963	0.7045	0.0067	0.0041	0.4963	51.1738	60.5239	0.0436	-0.4344
Darkhair	40408	0.5013	0.7080	0.0713	0.0046	0.5013	51.1299	59.3311	-0.0283	-0.425
Fish	39801	0.488	0.6986	0.0612	0.0053	0.488	51.2468	63.9927	-0.0516	-0.4072
Frog	35655	0.4998	0.7070	0.0063	0.0041	0.4998	51.1425	67.009	0.0057	-0.4308
Goldhill2	43237	0.4989	0.7063	0.0096	0.0044	0.4989	51.1505	59.5063	0.0729	-0.416
House	35878	0.3683	0.6069	0.1732	0.0027	0.3683	52.4692	60.6775	0.1353	-0.2998
Jetplane	11545	0.4991	0.7065	0.0157	0.0028	0.4991	51.1493	55.0727	0.0361	-0.4773
Lake	32667	0.4997	0.7069	0.0066	0.004	0.4997	51.144	64.0182	-0.0360	-0.4373
Lena	31227	0.4998	0.7070	0.0154	0.004	0.4998	51.1428	59.1577	0.0209	-0.4394
Library	28315	0.5983	0.7735	0.0016	0.0041	0.5983	50.362	58.3347	-0.0422	-0.5459
Lighthouse	40906	0.5031	0.7093	0.0033	0.0044	0.5031	51.1143	60.5441	0.0661	-0.425
Man	35528	0.5012	0.7080	0.0078	0.0045	0.5012	51.1306	58.645	0.0046	-0.4329
Mandril gray	30728	0.5017	0.7083	0.0077	0.0039	0.5017	51.1267	64.7751	0.0009	-0.4416
Palehair	22802	0.5039	0.7099	0.0049	0.0037	0.5039	51.1071	61.7554	0.0450	-0.4614
Pentagon	19534	0.5046	0.7104	0.0042	0.0036	0.5046	51.1011	63.5935	0.0068	-0.4668
Pepper	33117	0.4913	0.7009	0.0068	0.0042	0.4913	51.2173	58.1202	-0.0195	-0.4238
Rice	45744	0.4996	0.7068	0.0513	0.0045	0.4996	51.1447	62.2896	0.0587	-0.412
Walkbridge	39859	0.4982	0.7058	0.0032	0.0044	0.4982	51.1569	63.1365	0.1072	-0.4204
clown	49431	0.4131	0.6427	0.01	0.0061	0.4131	51.97	54.6714	0.0584	-0.2924
mountain	29538	0.5029	0.7092	0.0013	0.0036	0.5029	51.1163	60.3184	0.0285	-0.447
washsat	62489	0.4745	0.6888	0.0233	0.0072	0.4745	51.3688	55.1983	0.0045	-0.3463
zelda	48486	0.5004	0.7074	0.0342	0.0055	0.5004	51.1381	58.2598	-0.0107	-0.4076

Mean of Normalized Cross-Correlation (NCC) is tabulated above

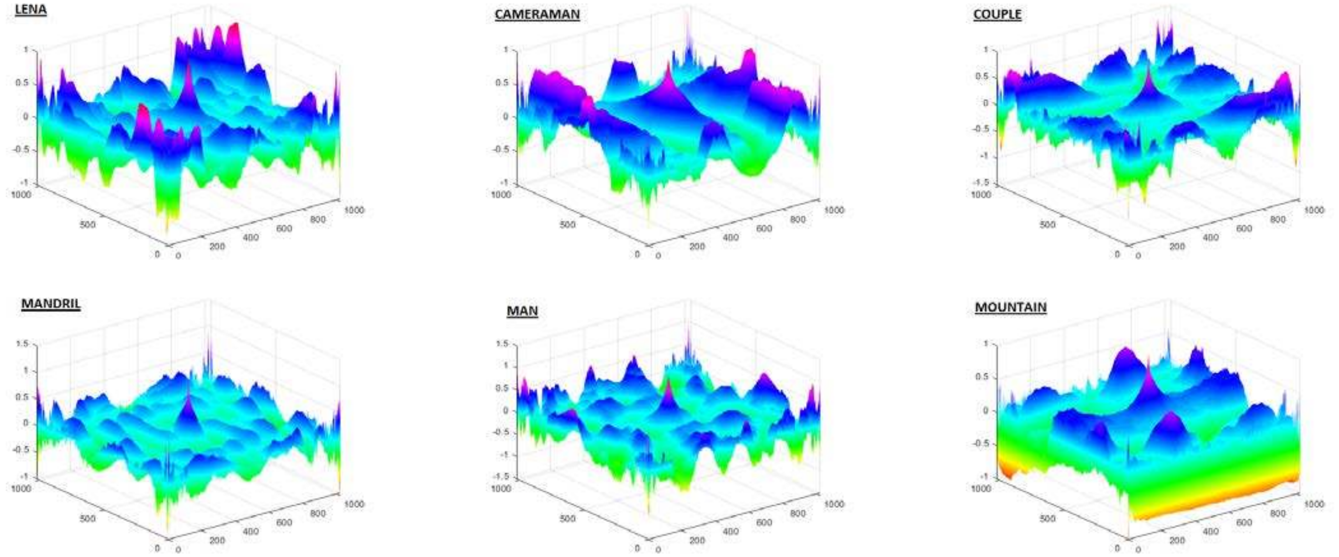


Fig. 13. Normalized Cross-Correlation Illustrated for some Popular Images.

In image processing (IP), the mean of an Image often termed as spatial filtering is used for noise reduction. Standard Deviation (STD), on the other hand, accounts for the variation or dispersion from the average mean, or anticipated value. A low STD means that the image pixels tend to be closer to the mean, whereas a higher value indicates that the pixels are spread over a broad range of values. For Stego images, the mean and the STD tell on the noise and change in the luminance/intensity of the pixel values. Table III gives a comparison of the mean and STD of the cover images used in testing our proposed methodology.

C. Reduced-Reference Test Results

Reduced-reference Image Quality Assessment was carried out in purview of [57] and conjunction with MATLAB GitHub repository. The results rendered for the test images are as shown in Table IV. It is pertinent to mention that lower the quality score (QS), the higher is the Stego-image quality.

D. No Reference/Blind IQA Test Results

It tends to build a computational model to predict the subjective quality quantitatively from the partisan image without having the aid of original or reference copy. Functions, namely BRIQE, NIQE, and PIQE that accept the distorted/Stego-image as input are used for the computational purpose. Table IV summarizes the output quality scores for the said IQA's. Note that for PIQE, high perceptual quality is associated with a low score value, whereas a high score means low perceptual quality. For NIQE, the case is just the opposite of PIQE.

E. Comparative Analysis

Undoubtedly, the sequential LSB replacement is a security threat, as pointed out by [66]. LSB Steganography is also undermined to have structural flaws [97] and in offering a weak association between consecutive bit planes [98]. However, LSB Steganography, until today, is a strong contender amongst its counterparts. The said fact is evident from Table V that demonstrates high structural similarity and less interference for our proposed secure bit embedding algorithm. The data for the said table is from the recently published [99], which has referred to the studies of [100–102].

Other recent work, including [103], [104] for blending pixel-value difference (PVD) and LSB techniques, and local binary pattern-based (LBPB) [105], published findings that are contrasted in Table VI, further expounds on higher PSNR values as rendered by our proposed bit embedding methodology.

TABLE III. REDUCED REFERENCE (RR) & NO/BLIND REFERENCE (NR) IQA

Test Images	Maximum		Structural Similarity			R. Ref.	No Reference - IQA		
	M. Bits	bpp	SSIM	MSSIM	SC	RRIQA	BRISQE	NIQE	PIQE
APC Aerial Airplane Barbra Boat Breakfast Cameraman Cars and APC Couple Darkhair Fish Frog Goldhill2 House Jetplane Lake Lena Library Lighthouse Man Mandril gray Palehair Pentagon Pepper Rice Walkbridge clown mountain washsat zelda	17146	0.0654	0.9986	0.9995	0.9961	0.8093	27.233	5.3995	13.6299
	6127	0.0234	0.999	0.9998	0.9948	0.9883	12.2286	2.7113	22.4038
	2431	0.0093	0.9972	0.9992	0.9952	2.3488	16.6887	5.7391	21.7968
	37875	0.1445	0.9981	0.9996	0.9932	0.5127	31.8209	4.6049	33.0083
	18691	0.0713	0.9979	0.9996	0.994	1.5277	6.9412	5.0183	18.2527
	14939	0.0570	0.9987	0.9998	0.995	0.9059	41.539	5.4934	51.7844
	25641	0.0978	0.997	0.9993	0.9937	1.6629	33.0189	5.1635	41.3617
	44159	0.1685	0.9989	0.9997	0.9933	0.3350	9.9519	4.1246	20.3461
	32239	0.1230	0.9985	0.9997	0.9934	1.1657	28.2067	3.362	25.824
	40427	0.1542	0.9966	0.9993	0.9936	1.4869	20.5537	4.0567	20.368
	39820	0.1519	0.9967	0.9989	0.9934	0.7906	41.5285	4.0947	65.3779
	35674	0.1361	0.9987	0.9997	0.9933	0.6727	19.1534	4.0332	24.3395
	43256	0.1650	0.9983	0.9997	0.9935	1.1303	13.7579	3.5827	18.5686
	35897	0.1369	0.9978	0.9995	0.9968	1.1906	52.6812	4.4929	46.2368
	11564	0.0441	0.9977	0.9995	0.9949	1.5764	26.5814	3.1438	21.7911
	32686	0.1247	0.9983	0.9996	0.9941	0.8629	21.7387	4.36	19.3017
	31246	0.1192	0.9976	0.9995	0.9936	1.4719	4.8896	4.2099	17.0984
	28334	0.1081	0.9992	0.9998	0.9935	0.9255	42.1952	4.2689	48.093
	40925	0.1561	0.9985	0.9996	0.9937	1.2733	18.636	2.9754	38.8563
	35547	0.1356	0.9981	0.9996	0.9931	0.5882	23.1349	2.8212	21.3023
	30747	0.1173	0.999	0.9998	0.9935	0.6472	51.9592	7.9671	22.9831
	22821	0.0871	0.998	0.9996	0.9936	1.3137	18.5818	4.8185	22.3224
	19553	0.0746	0.9988	0.9998	0.9934	0.8922	15.1769	4.6506	16.8965
	33136	0.1264	0.9984	0.9995	0.9934	1.3861	35.5626	7.288	27.3557
	45763	0.1746	0.9977	0.9996	0.9933	1.0565	35.7323	7.1433	24.1532
	39878	0.1521	0.9991	0.9998	0.9937	0.7311	9.5149	2.5131	28.9098
	49450	0.1886	0.9979	0.9992	0.994	1.2194	21.7439	4.8926	43.1609
	29557	0.1128	0.9986	0.9995	0.9948	1.0588	15.9205	3.0943	38.3954
	62508	0.2384	0.9971	0.9992	0.9896	0.9676	9.8024	4.185	18.5335
	48505	0.1850	0.9972	0.9995	0.9923	1.2972	19.0354	5.6148	11.2756

TABLE IV. CONTRASTING FR-IRQ OF THE PROPOSED ALGO

Test Image	Reference	MSE	MAE	PSNR	NCC	SSIM
Airplane	[36]	0.47	N/A	51.36	N/A	0.9957
	[106]	1.3211	0.6107	41.5506	0.99999	0.9831
	Proposed	0.4334	0.4334	51.7619	0.07	0.9972
Baboon	[36]	0.51	N/A	51.01	N/A	0.9995
	[106]	0.4284	0.2244	48.8172	1	N/A
	Proposed	0.5017	0.5017	51.1267	0.0009	0.999
Barbara	[36]	0.52	N/A	50.94	N/A	0.999
	[106]	0.3442	0.1656	49.6504	0.99999	N/A

	Proposed	0.5001	0.5001	51.1405	0.0052	0.9981
Boat	[36]	0.46	N/A	51.41	N/A	0.9989
	Proposed	0.4907	0.4907	51.2224	0.1088	0.9979
Car man	[106]	0.2211	0.2221	51.6788	0.99999	N/A
	Proposed	0.5002	0.5002	51.1392	0.0955	0.997
Lena	[36]	0.52	N/A	50.95	N/A	0.999
	[106]	0.1014	0.1146	55.0332	0.99999	0.9684
	Proposed	0.4998	0.4998	51.1428	0.0209	0.9976
Peppers	[36]	0.9765	N/A	47.5	N/A	0.9579
	[106]	0.4585	0.2907	46.6995	0.99998	0.9706
	Proposed	0.4913	0.4913	51.2173	-0.0195	0.9984

TABLE V. A COMPARISON WITH SOME OTHER POPULAR STEGANOGRAPHY TECHNIQUES

Images	Test Parameters	**PVD [100]**	**TBPC [101]**	**ATBPC [102]**	**ATCEQES [99]**	**Proposed Method**
Lena	**PSNR**	52.51	53.34	55.34	56.49	51.1428
	WPSNR	67.41	67.45	67.45	72.47	59.1577
	SSIM	0.9982	0.9987	0.9987	0.9999	0.9976
Baboon	**PSNR**	52.23	55.3	55.3	56.49	51.1267
	WPSNR	86.58	79.55	79.55	84.82	64.7751
	SSIM	0.9993	0.9995	0.9995	0.999	0.9990
Cameraman	**PSNR**	53.03	55.3	55.31	56.47	51.1392
	WPSNR	66.9	65.32	66.01	63.92	60.2802
	SSIM	0.9978	0.9983	0.9984	0.9999	0.9997
Peppers	**PSNR**	52.49	55.39	55.38	56.51	51.2173
	WPSNR	67.63	68.49	68.84	70.65	58.1202
	SSIM	0.9984	0.9988	0.9988	0.9999	0.9984

TABLE VI. A COMPARISON OF PSNR RENDERED BY PVD+ LSB AND FREQUENCY DOMAIN STEGANOGRAPHY ALGOS

Stego Image	**LBPB [105]**	**PVD [104]**	**3LSB [104]**	**PVD+LSB [103]**	**Frequency Domain[103]**	**Proposed Method**
Lena	56.82	39.56	37.92	36.32	45.05	51.1428
Baboon	53.57	37.38	37.93	35.4	41.82	51.1267
Peppers	58.64	39.11	37.93	35.91	45.65	51.2173
Jet	56.23	39.12	37.94	36.41	44.77	51.1493
Boat	57.95	N/A	N/A	35.72	45.7	51.2224
Lake	N/A	N/A	N/A	35.89	0	51.1445
Elaine	N/A	N/A	N/A	34	0	N/A
Couple	N/A	N/A	N/A	35.78	45.95	51.1738

IX. DISCUSSION

The comparison made in the preceding section is in the purview of the fact that the detection and extraction of hidden information are independent of the type of Steganography used and the misapprehension associated with its allied bit embedding capacity such as [106]. It is because the more the message bits embedded inside the cover, the greater shall be the threat of exposure of the underneath bit embedding algorithm. Moreover, changing cover bits in proportion to the message bits may also reveal the hidden content length. More importantly, the reusability of cover images may lead to a compromised situation. As regards images, what matters most at a glance is the perceptibility of the Stego image, which, however, is dependent on the perception of the onlooker/attacker. Practically, subjective image analysis is almost impossible because millions of images are uploaded each day on the web [107]. Hence, a combination of all the theoretical/subjective and objective image analysis techniques contributes to the acceptance or otherwise of any image-based Steganography technique. It is, therefore, imperative to quantify the results of each technique through some Universal rating into a quality score to assess and grade any Steganographic method. It shall help uphold the impartiality by removing the bias towards self-proclaimed efficiency and the effectiveness of one's proposed Steganography method.

For instance, take the example of an original image having an MSE = 0 and an SSIM = 1, as shown in Fig. 14 adapted from [108]. It is apparent from Fig. 15 that despite having the same MSE = 144, the structural distortion in the images is quite visible/easily detectable. Moreover, different images can have the same PSNR, SSIM, and even entropy. For a thorough understanding, [109] is a good starting point.

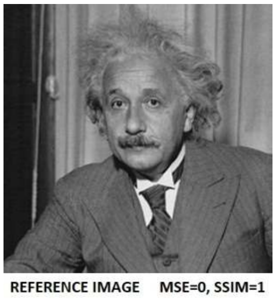


Fig. 14. Original. MSE = 0; SSIM = 1 [108].

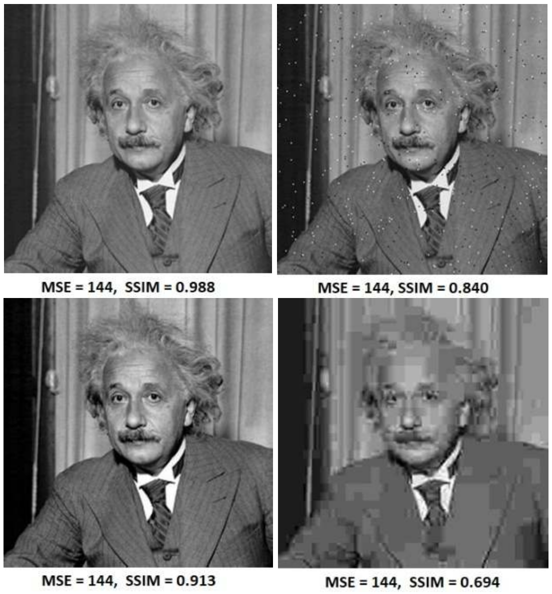


Fig. 15. Deceptive Statistics for MSE = 144. Adapted from [108].

While [110] stating Watermarking techniques as belonging to a particular group of the Steganography field indicated a trade-off between the three gauging parameters of imperceptibility, capacity, and the robustness as regards watermark system. That is, increased payload shall likely distort the quality of the image. In contrast, the requirement of being secured against Steganalysis also depends on the depth of the embedded bits as LSB, 2-LSB, and such other choices. Likewise, to increase the quality of the Stego image, one needs to either lessen the amount of data to be hidden or the depth of the embedded bits, which seems the main reason behind recent studies for publishing results to 30 or 50% LSB bit embedding. However, as far as the strength of any proposed LSB Steganography bit embedding algorithm goes, it needs to be tested against its full capacity that is 100% bit embedding to get an unbiased view on its security, capacity, and imperceptibility aspects. Our test results are within the purview of [111] that explicitly stated as "excellent", a PSNR with 53 for 100% embedding (1bit per pixel), and calls for the test image 'Lena,' a PSNR value of ≥ 50.

Another distinct limitation noticed while reviewing the literature of state-of-of-the-art image Steganography techniques is that the least emphasis is given to the Steganalysis that gauges the security/limitations of the bit embedding methodology without which the discussion of data obliviousness through Steganography remains incomplete. Table VII contrasting the Steganalysis results with the recent research [36], which is for images of size 128 × 128 as compared to our proposed that are carried out on 512 × 512 images, each with a depth of 8-bits.

TABLE VII. A COMPARISON OF RS AND SP STEGANALYSIS BETWEEN [36] AND THE PROPOSED METHOD BETWEEN [36] AND THE PROPOSED METHOD.

	[36]		Proposed		
	128 x 128		512	x	512
	RS	SP	RS	SP	
Airplane	0.0603	0.0710	0.0048	-0.0109	
Barbra	0.0576	0.0448	0.2975	0.2064	
Boat	0.1120	0.1365	0.1258	0.0207	
Lena	0.0170	0.0569	0.1372	0.2942	
Mandril	0.4919	0.4653	0.3758	0.1408	

A. Theoretical Facet

Kerckhoff (1883) stated the principle of security for a cryptographic system, which could easily be extended to Steganography as well. According to Kerckhoff, the security of a public domain cryptographic system resides in its secret key. Likewise, for digital Steganography to work effectively, there must exist some surreptitious bit manipulation mechanism because otherwise contrasting the cover and Stego object shall expose the hidden secret.

- Example: Let *s* denotes the Stego object computed by some function *γs* by taking some cover *c* and the payload *m*, then the bit embedding *γs* and extraction *ξe* processes can be expressed as shown in Eq. 22:

$$\left.\begin{array}{l} \text{\%Stego Object} \\ s = \gamma s(c, m) \\ \text{\% Extracting Message Bits from Cover Image} \\ c' = \xi e(s) \\ \quad = \xi e(\gamma s(c, m)) \\ m' = (c, c')? \end{array}\right\} \qquad (22)$$

Interestingly, the above also holds (partially or in full) with the introduction of Stego key *k* with known cover and the Stego object, shown in Eq. 23. Additionally, with the same cover, it may also unconsciously lead to a Stego key compromise as well.

$$\left.\begin{array}{l} s = \gamma s(c, k, m) \\ c' = \xi e(s) \\ c' = \xi e(\gamma s(c, k, m)) \\ m' = (c, c')_k\ ? \\ \quad = m \text{ (message segment(s) or full message)} \end{array}\right\} \qquad (23)$$

It follows from Eq. 23 that the mutual information $I_m(c; s)$ explains on the information about *c* if *s* is known, as shown in Eq. 24, with H(*c*), and H(*c*|*s*) being the respective entropies:

$$\mathrm{I}(c;\, s) = \mathrm{H}(c) - \mathrm{H}(c|s) \tag{24}$$

Eq. 24 equally holds when the secret information (say) E gets embedded inside the cover *c,* as shown in Eq. 25.

$$I(E, (c, s)) = H(E) - H(E|(c, s)) \tag{25}$$

Eq. (25) implies that security objectives can not be met when both cover and Stego object is known or unless Eqn. (26) equates to zero:

$$I(E, (c, s)) = 0 \tag{26}$$

It follows from above that a technically viable solution would then need a dynamic indeterministic bit embedding mechanism capable of giving different results on each of its occurrences, as shown in Eq. 27.

$$\left.\begin{array}{l} \%\text{Stego Object} \\ s = \gamma s(c,\, r,\, k,\, m/r \leftarrow \textit{condition for substitution}) \\ \%\ \text{Extracting Message Bits from Cover Image} \\ m = \xi e(s) \\ = \xi e(\gamma s(c,\, k,\, m/r \leftarrow \textit{conditonal extraction})) \\ = [r \text{ or } m]\ \text{// uncertanity in predicting } r \text{ and } m \end{array}\right\} \tag{27}$$

, where the Stego key k is different for every new message.

It is evident from Eq. (27) that security lies in disconnecting the one-to-one/linear mapping of cover bits with those of the message bits through some unpredictable phenomena during the bit embedding process.

In practice, TRNGs are known to provide unpredictable results each time these get executed, and the information theory also supports the concept of randomness.

Based on the above analogy, our proposed bit embedding methodology remains novel amongst the recently suggested Image-based secure Steganography solutions.

X. Conclusion

In today's world, it is difficult to remain isolated from the digitalization progression that is doubling the data every two years. Hence, regardless of the willful or unconscious data generation, its protection from unauthorized exposure and illegal usage remains the primary concern of information security forefront. In this regard, several information hiding techniques have poured in. Still, the most significant and widely adopted amongst those is that of digital image Steganography because of its aptness in deceiving the human visual system and the redundancy of picture elements to serve as place holders for secret bit embedding. However, recent studies seem short in considering and addressing to its full, the security aspects of Steganalysis, detectability of embedded bits through known cover and known message attack, using Stego key while proposing such furtive schemes or aligning those to information-theoretic perspective. Misconception regarding mean square error (MSE) and peak signal to noise ratio (PSNR) are visible in the tests conducted, which are preferred over the structural similarity index (SSIM). Much of the effort rests in increasing bit hiding capacity in place of squeezing the critical contents to avoid compromise of underneath bit embedding methodology or facilitating in the reusability of the same cover for multiple communication. This research endeavor attempts to subdue the above-cited limitations by suggesting an information-theoretic secure secret bit embedding Steganography solution through the use of a TRNG. An explicit take away of the proposed study is that the security of LSB Steganography lies in disconnecting the consecutive replacement of secret message bits by inducing uncertainty in the bit embedding process. An implicit assertion of the proposed research is to highlight the need and significance of standardization of the quality scores to remove bias in gauging newly evolved or enhanced Image-based Steganography solution for Universal acceptance.

References

[1] A. A. Kharlamov and G. Parry," The impact of servitization and digitization on productivity and profitability of the firm: a systematic approach," Production Planning & Control, pp. 1-13, 2020.

[2] S. S. Arslan, R. Jurdak, J. Jelitto, and B. Krishnamachari," Advancements in distributed ledger technology for Internet of Things," ed:Elsevier, 2020.

[3] M. Wairiya, A. Shah, and G. Sahu," Mobile Learning Adoption: An Empirical Study," in 2020 10th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 2020, pp. 757-761.

[4] R. Ernst and J. Haar," Competitiveness," in Globalization, Competitiveness, and Governability, ed: Springer, 2019, pp. 47-67.

[5] M. Jozani, E. Ayaburi, M. Ko, and K.-K. R. Choo," Privacy concerns and benefits of engagement with social media-enabled apps: A privacy calculus perspective," Computers in Human Behavior, vol. 107, p.106260, 2020.

[6] Gartner," Gartner Says Data and Cyber-Related Risks Remain Top Worries for Audit Executives," 2019.

[7] P. Shukla, H. Kazemian, F. FIET, and C. Eng," Privacy in The First Line of the First Code," Science Magazine, vol. 17, p. 04, 2020.

[8] K. Sanjeev, B. Janet, and R. Eswari," Automated Cyber Threat Intelligence Generation from Honeypot Data," in Inventive Communication and Computational Technologies, ed: Springer, 2020, pp. 591-598.

[9] A. Stetsenko," Transformative-Activist and Social Justice Approaches to the History of Psychology," in Oxford Research Encyclopedia of Psychology, ed, 2020.

[10] V. Kvashis and Y. Sluchevskaya," Limits of Acceptable State Interference in Privacy," in XVII International Research-to-Practice Conference dedicated to the memory of MI Kovalyov (ICK 2020), 2020, pp. 255-258.

[11] Y. Lu and S. Li," From data flows to privacy issues: a user-centric semantic model for representing and discovering privacy issues," in Proceedings of 53rd Hawaii International Conference on System Sciences, 2020.

[12] O. A. Al-Harbi, W. E. Alahmadi, and A. O. Aljahdali," Security analysis of DNA based Steganography techniques," SN Applied Sciences, vol. 2, pp. 1-10, 2020.

[13] A. Singh," Cryptography: A Never Ending Technology," CYBERNOMICS, vol. 2, pp. 45-47, 2020.

[14] M. G. Vigliotti and H. Jones," Cryptography for Busy People," in The Executive Guide to Blockchain, ed: Springer, 2020, pp. 23-40.

[15] R. Shanthakumari and S. Malliga," Dual layer security of data using LSB inversion image Steganography with elliptic curve cryptography encryption algorithm," Multimedia Tools and Applications, vol. 79, pp. 3975-3991, 2020.

[16] D. John F," Review of The Third Reich is Listening by Christian Jennings," Cryptologia, vol. 44, pp. 91-95, 2020.

[17] O. Rachael, S. Misra, R. Ahuja, A. Adewumi, F. Ayeni, and R.Mmaskeliunas," Image Steganography and Steganalysis Based on Least Significant Bit (LSB)," in Proceedings of ICETIT 2019, ed:Springer, 2020, pp. 1100-1111.

[18] N. T. Courtois, M.-B. Oprisanu, and K. Schmeh," Linear cryptanalysis and block cipher design in East Germany in the 1970s," Cryptologia, vol. 43, pp. 2-22, 2019.

[19] N. T. Courtois and M. Georgiou," Constructive non-linear polynomial cryptanalysis of a historical block cipher," arXiv preprint arXiv:1902.02748, 2019.

[20] G. Wu, F. Zhang, L. Shen, F. Guo, and W. Susilo," Certificateless aggregate signature scheme secure against fully chosen-key attacks," Information Sciences, vol. 514, pp. 288-301, 2020.

[21] M. Bouam, C. Bouillaguet, and C. Delaplace," Brute-Force Cryptanalysis with Aging Hardware: Controlling Half the Output of SHA-256," 2019.

[22] S. Khatoon and B. Singh Thakur," Cryptanalysis and improvement of authentication scheme for roaming service in ubiquitous network," Cryptologia, pp. 1-26, 2020.

[23] C. B. Smith," The Comparison of Steganography and Cryptography:Concealing Information," Utica College, 2019.

[24] N. F. Johnson and S. Jajodia," Exploring Steganography: Seeing the unseen," Computer, vol. 31, pp. 26-34, 1998.

[25] R. J. Anderson and F. A. Petitcolas," On the limits of Steganography," IEEE Journal on selected areas in communications, vol. 16, pp. 474-481, 1998.

[26] S. Arunkumar, V. Subramaniyaswamy, V. Vijayakumar, N. Chilamkurti, and R. Logesh," SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images," Measurement, vol. 139, pp. 426-437, 2019.

[27] "Definitions.", LIA - Laboratory of Advanced Research on Computer Science, 2020.

[28] R. Gonzalez and R. Woods," Digital Image Processing 3rd edn Pearson Prentice Hall," 2008.

[29] S. Boutnaru," Steganography obsfucation," ed: Google Patents, 2020.

[30] H.-C. Wu, N.-I. Wu, C.-S. Tsai, and M.-S. Hwang," Image steganographic scheme based on pixel-value differencing and LSB replacement methods," IEE Proceedings-Vision, Image and Signal Processing, vol. 152, pp. 611-615, 2005.

[31] R. Kavitha, U. Eranna, and M. Giriprasad," DCT-DWT Based Digital Watermarking and Extraction using Neural Networks," in 2020 International Conference on Artificial Intelligence and Signal Processing (AISP), 2020, pp. 1-5.

[32] A. Jalali and H. Farsi," A new Steganography algorithm based on video sparse representation," Multimedia Tools and Applications, vol.79, pp. 1821-1846, 2020.

[33] C. W. Kurak Jr and J. McHugh," A cautionary note on image downgrading," in ACSAC, 1992, pp. 153-159.

[34] D. Ghosh, A. K. Chattopadhyay, K. Chanda, and A. Nag," A Secure Steganography Scheme Using LFSR," in Emerging Technology in Modelling and Graphics, ed: Springer, 2020, pp. 713-720.

[35] C. Pak, J. Kim, K. An, C. Kim, K. Kim, and C. Pak," A novel color image LSB Steganography using improved 1D chaotic map," Multimedia Tools and Applications, vol. 79, pp. 1409-1425, 2020.

[36] A. Chatterjee, S. K. Ghosal, and R. Sarkar," LSB based Steganography with OCR: an intelligent amalgamation," Multimedia Tools and Applications, pp. 1-19, 2020.

[37] M. A. Al Mamun, S. M. Alam, M. S. Hossain, and M. Samiruzzaman," A Novel Image Steganography Using Multiple LSB Substitution and Pixel Randomization Using Stern-Brocot Sequence," in Future of Information and Communication Conference, 2020, pp. 756-773.

[38] N. Soni, I. Saini, and B. Singh," Integer Wavelet Transform-Based ECG Steganography for Hiding Patients' Confidential Information in e-Healthcare Systems," in Soft Computing: Theories and Applications, ed: Springer, 2020, pp. 513-525.

[39] A. K. Sahu and G. Swain," Reversible Image Steganography Using Dual-Layer LSB Matching," Sensing and Imaging, vol. 21, p. 1, 2020.

[40] A. Jain," A Secured Steganography Technique for Hiding Multiple Images in an Image Using Least Significant Bit Algorithm and Arnold Transformation," in International Conference on Intelligent Data Communication Technologies and Internet of Things, 2019, pp. 373-380.

[41] B. Praveen, D. Samanta, G. Prasad, C. R. Kumar, and M. Prasad," Protecting Medical Research Data Using Next Gen Steganography Approach," in International Conference on Information, Communication and Computing Technology, 2019, pp. 340-348.

[42] A. Saikia and T. Tuithung," A Novel True Colour Image Bit Modification Technique for Image Steganography," in International Conference on Soft Computing and Signal Processing, 2019, pp. 317-327.

[43] N. S. R. Chandra, V. Sneha, and P. V. Paul," A Novel Image Steganography Model Using LSB with Extended ASCII Codes," in Smart Intelligent Computing and Applications, ed: Springer, 2020, pp.107-116.

[44] G. Luo, R.-G. Zhou, and Y. Mao," Two-level information hiding for quantum images using optimal LSB," Quantum Information Processing, vol. 18, p. 297, 2019.

[45] B. Datta, S. Roy, S. Roy, and S. K. Bandyopadhyay," Multi-bit robust image Steganography based on modular arithmetic," Multimedia Tools and Applications, vol. 78, pp. 1511-1546, 2019.

[46] D. Nashat and L. Mamdouh," An efficient steganographic technique for hiding data," Journal of the Egyptian Mathematical Society, vol. 27, pp. 1-14, 2019.

[47] P. Artiemjew and A. Kislak-Malinowska," Using r-indiscernibility Relations to Hide the Presence of Information for the Least Significant Bit Steganography Technique," in International Conference on Information and Software Technologies, 2019, pp. 209-220.

[48] N. M. Al-Aidroos and H. A. Bahamish," Image Steganography Based on LSB Matching and Image Enlargement," in 2019 First International Conference of Intelligent Computing and Engineering (ICOICE), 2019, pp. 1-6.

[49] A. K. Sahu and G. Swain," A novel n-rightmost bit replacement image Steganography technique," 3D Research, vol. 10, p. 2, 2019.

[50] Pichardo-M'endez, JL and Palacios-Luengas, L and Mart' ınez-Gonz'alez, RF and Jim' enez-Ram 'ırez, O and V'azquez-Medina, R," LSB Pseudorandom Algorithm for Image Steganography Using Skew Tent Map," Arabian Journal for Science and Engineering, pp. 1-20, 2019.

[51] I. Maurya and S. Gupta," Inverted LSB Image Steganography," in Soft Computing: Theories and Applications, ed: Springer, 2020, pp. 19-29.

[52] G. Swain," Very high capacity image Steganography technique using quotient value differencing and LSB substitution," Arabian journal for science and engineering, vol. 44, pp. 2995-3004, 2019.

[53] P. Agarwal, D. Moudgil, and S. Priya," Encrypted Transfer of Confidential Information Using Steganography and Identity Verification Using Face Data," in Artificial Intelligence and Evolutionary Computations in Engineering Systems, ed: Springer, 2020, pp. 155-166.

[54] A. Kerckhoffs," La cryptographie militaire. 9: 5–38," ed: January, 1883.

[55] J. Von Neumann," 13. various techniques used in connection with random digits," Appl. Math Ser, vol. 12, p. 5, 1951.

[56] G. J. Simmons," The prisoners' problem and the subliminal channel," in Advances in Cryptology, 1984, pp. 51-67.

[57] Z. Wang and E. P. Simoncelli," Reduced-reference image quality assessment using a wavelet-domain natural image statistic model," in Human Vision and Electronic Imaging X, 2005, pp. 149-159.

[58] J. Z¨ollner, H. Federrath, H. Klimant, A. Pfitzmann, R. Piotraschke, A. Westfeld, et al., ”Modeling the security of steganographic systems,” in International Workshop on Information Hiding, 1998, pp. 344-354.

[59] J. Wen, X. Zhou, P. Zhong, and Y. Xue," Convolutional neural network based text steganalysis," IEEE Signal Processing Letters, vol. 26, pp.460-464, 2019.

[60] H. Lee and H.-W. Lee," New Approach on Steganalysis: Reverse-Engineering based Steganography SW Analysis," in Proceedings of the 2020 9th International Conference on Software and Computer Applications, 2020, pp. 212-216.

[61] F. Nabi," A Survey on Image Steganography." academia.edu

[62] S. Trivedi and R. Chandramouli," Active steganalysis of sequential Steganography," in Security andWatermarking of Multimedia Contents V, 2003, pp. 123-130.

[63] J. Kelley," Terror groups hide behind Web encryption," USA today, vol. 5, p. 2001, 2001.

[64] J. Cosic and M. Baˇca," Steganography and steganalysis-does local web sites contain "Stego" contents?," in Proceedings ELMAR-2010, ed, 2010.

[65] G. Rajput and R. Agrawal," Evaluation of feature selection measures for Steganalysis," in International Conference on Pattern Recognition and Machine Intelligence, 2009, pp. 432-439.

[66] A. D. Ker," A general framework for structural Steganalysis of LSB replacement," in International Workshop on Information Hiding, 2005, pp. 296-311.

[67] J. Fridrich and M. Goljan," On estimation of secret message length in LSB Steganography in spatial domain," in Security, Steganography, and watermarking of multimedia contents VI, 2004, pp. 23-34.

[68] A. D. Ker and R. B¨ohme," Revisiting weighted Stego-image Steganalysis," in Security, Forensics, Steganography, and Watermarking of Multimedia Contents X, 2008, p. 681905.

[69] A. Westfeld and A. Pfitzmann," Attacks on steganographic systems," in International workshop on information hiding, 1999, pp. 61-76.

[70] O. Dabeer, K. Sullivan, U. Madhow, S. Chandrasekaran, and B. Manjunath," Detection of hiding in the least significant bit," IEEE Transactions on Signal Processing, vol. 52, pp. 3046-3058, 2004.

[71] S. Dumitrescu, X. Wu, and N. Memon," On Steganalysis of random LSB embedding in continuous-tone images," in Proceedings. International Conference on Image Processing, 2002, pp. 641-644.

[72] L. Fillatre," Adaptive Steganalysis of least significant bit replacement in grayscale natural images," IEEE Transactions on Signal Processing, vol. 60, pp. 556-569, 2011.

[73] M. A. Alsmirat, R. A. Al-Hussien, W. a. T. Al-Sarayrah, Y. Jararweh, and M. Etier," Digital video forensics: a comprehensive survey," International Journal of Advanced Intelligence Paradigms, vol. 15, pp.437-456, 2020.

[74] L. A. Sandoval-Bravo, V. I. Ponomaryov, R. Reyes-Reyes, and C.Cruz-Ramos," Coverless image Steganography framework using distance local binary pattern and convolutional neural network," in Real-Time Image Processing and Deep Learning 2020, 2020, p. 114010D.

[75] A. Gutub and F. Al-Shaarani," Efficient Implementation of Multiimage Secret Hiding Based on LSB and DWT Steganography Comparisons," Arabian Journal for Science and Engineering, pp. 1-14, 2020.

[76] T. Sudhakar, S. S. V. Sriraman, and N. Venkateswaran," Synthesis and Evaluation of Improved Reference Matrix Models for High Capacity Image Steganography," in 2020 International Conference on Artificial Intelligence and Signal Processing (AISP), 2020, pp. 1-6.

[77] T. Rabie, M. Baziyad, and I. Kamel," High Payload Steganography:Surface-Fitting The Transform Domain," in 2019 International Conference on Communications, Signal Processing, and their Applications (ICCSPA), 2019, pp. 1-6.

[78] U. Pilania and P. Gupta," A Proposed Optimized Steganography Technique using ROI, IWT and SVD," International Journal of Information Systems & Management Science, Forthcoming, 2019.

[79] S. J. Gladwin and P. L. Gowthami," Combined Cryptography and Steganography for Enhanced Security in Suboptimal Images," in 2020 International Conference on Artificial Intelligence and Signal Processing (AISP), 2020, pp. 1-5.

[80] H. S. Radeaf, B. M. Mahmmod, S. H. Abdulhussain, and D. Al-Jumaeily," A Steganography based on orthogonal moments," in Proceedings of the International Conference on Information and Communication Technology, 2019, pp. 147-153.

[81] A. R. Idrais, S. Harb, M. O. Ahmad, and M. Swamy," A Novel High Capacity Data Hiding Algorithm using Salt and Pepper Noise," in 2020 11th International Conference on Information and Communication Systems (ICICS), 2020, pp. 131-135.

[82] X. Duan, D. Guo, N. Liu, B. Li, M. Gou, and C. Qin," A New High Capacity Image Steganography Method Combined With Image Elliptic Curve Cryptography and Deep Neural Network," IEEE Access, vol. 8, pp. 25777-25788, 2020.

[83] A. Seif and W. Alexan," A High Capacity Gray Code Based Security Scheme for Non-Redundant Data Embedding," in 2020 International Conference on Innovative Trends in Communication and Computer Engineering (ITCE), 2020, pp. 130-136.

[84] W. Liu, X. Yin, W. Lu, J. Zhang, J. Zeng, S. Shi, et al.," Secure halftone image Steganography with minimizing the distortion on pair swapping," Signal Processing, vol. 167, p. 107287, 2020.

[85] J. Greffier, J. Frandon, A. Larbi, J. Beregi, and F. Pereira," CT iterative reconstruction algorithms: a task-based image quality assessment," European radiology, vol. 30, pp. 487-500, 2020.

[86] A. K. Moorthy and A. C. Bovik," Visual quality assessment algorithms:what does the future hold?," Multimedia Tools and Applications, vol. 51, pp. 675-696, 2011.

[87] L. Zhang, L. Zhang, X. Mou, and D. Zhang," A comprehensive evaluation of full reference image quality assessment algorithms," in 2012 19th IEEE International Conference on Image Processing, 2012, pp. 1477-1480.

[88] B. Lakshmi Sirisha," Image Steganography based on SVD and DWT techniques," Journal of Discrete Mathematical Sciences and Cryptography, pp. 1-8, 2020.

[89] S. T. Abdulrazzaq, M. M. Siddeq, and M. A. Rodrigues," A novel Steganography approach for audio files," SN Computer Science, vol. 1, pp. 1-13, 2020.

[90] W. Lyu, W. Lu, and M. Ma," No-Reference Quality Metric for Contrast-Distorted Image Based on Gradient Domain and HSV Space," Journal of Visual Communication and Image Representation, p.102797, 2020.

[91] A. Mittal, A. K. Moorthy, and A. C. Bovik," No-reference image quality assessment in the spatial domain," IEEE Transactions on image processing, vol. 21, pp. 4695-4708, 2012.

[92] A. Mittal, R. Soundararajan, and A. C. Bovik," Making a "completely blind" image quality analyzer," IEEE Signal Processing Letters, vol.20, pp. 209-212, 2012.

[93] N. Venkatanath, D. Praneeth, M. C. Bh, S. S. Channappayya, and S. S. Medasani," Blind image quality evaluation using perception based features," in 2015 Twenty First National Conference on Communications (NCC), 2015, pp. 1-6.

[94] A. Shnayderman, A. Gusev, and A. M. Eskicioglu," An SVD-based grayscale image quality measure for local and global assessment," IEEE transactions on Image Processing, vol. 15, pp. 422-429, 2006.

[95] C.-W. Kok and W.-S. Tam, Digital Image Interpolation in Matlab: John Wiley & Sons, 2019.

[96] U. Virtebi," The USC-SIPI Image Database."

[97] Ker, Andrew D and Pevn'y, Tom' aˇs and Kodovsk`y, Jan and Fridrich, Jessica," The square root law of steganographic capacity," in Proceedings of the 10th ACM workshop on Multimedia and security, 2008, pp. 107-116.

[98] T. Zhang and X. Ping," A new approach to reliable detection of LSB Steganography in natural images," Signal processing, vol. 83, pp. 2085-2093, 2003.

[99] A. Saeed, M. J. Khan, H. Shahid, S. I. Naqvi, M. A. Riaz, M. S. Khan, et al.," An Accurate Texture Complexity Estimation for Quality-Enhanced and Secure Image Steganography," IEEE Access, vol. 8, pp.21613-21630, 2020.

[100] S. S. Agrawal and R. M. Samant," Data hiding in grayscale images using pixel value differencing," in Technology Systems and Management, ed: Springer, 2011, pp. 27-33.

[101] R. Y. Li, O. C. Au, K. K. Lai, C. K. Yuk, and S.-Y. Lam," Data hiding with tree based parity check," in 2007 IEEE International Conference on Multimedia and Expo, 2007, pp. 635-638.

[102] H. Al-Dmour, N. Ali, and A. Al-Ani," An efficient hybrid Steganography method based on edge adaptive and tree based parity check," in International Conference on Multimedia Modeling, 2015, pp. 1-12.

[103] M. A. Hameed, M. Hassaballah, S. Aly, and A. I. Awad," An Adaptive Image Steganography Method Based on Histogram of Oriented Gradient

and PVD-LSB Techniques," IEEE Access, vol. 7, pp. 185189-185204, 2019.

[104] S. Prasad and A. K. Pal," Logistic map-based image Steganography scheme using combined LSB and PVD for security enhancement," in Emerging Technologies in Data Mining and Information Security, ed:Springer, 2019, pp. 203-214.

[105] S. Chakraborty and A. S. Jalal," A novel local binary pattern based blind feature image Steganography," Multimedia Tools and Applications, pp. 1-14, 2020.

[106] M. Nazari and I. D. Ahmadi," A novel chaotic Steganography method with three approaches for color and grayscale images based on FIS and DCT with flexible capacity," Multimedia Tools and Applications, pp. 1-32, 2020.

[107] N. K. Pandey and M. Diwakar," A Review on Cloud based Image Processing Services," in 2020 7th International Conference on Computing for Sustainable Global Development (INDIACom), 2020, pp.108-112.

[108] Z. Wang, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli," Image quality assessment: from error visibility to structural similarity," IEEE transactions on image processing, vol. 13, pp. 600-612, 2004. https://www.cns.nyu.edu/~lcv/ssim/

[109] Hor' e, A., and D. Ziou." Image quality metrics: PSNR versus SSIM." In Proceedings of the 2010 IEEE 20th International Conference on Pattern Recognition, vol. 1. 2010.

[110] A. Hanjalic, G. Langelaar, P. Van Roosmalen, J. Biemond, and R. Lagendijk, Image and video databases: restoration, watermarking and retrieval: Elsevier, 2000.

[111] Nag, Amitava. (2015). Re: What is the best PSNR value for the steganography method to hide the text in image?. Retrieved from: https://www.researchgate.net/post/What˙is˙the˙best˙PSNR˙value˙for˙the˙steganography˙method˙to˙hide˙the˙text˙in˙image/54e5a9d5d11b8b330b8b4581/citation/do- wnload.

AUTHOR’S PROFILE

Khan Farhan Rafat is a self-motivated individual having practical experience in the evolution, designing, and implementation of information security solutions together with formulation and drafting of allied security policies and procedures. He also possesses progressive experience in managing and securing IT operations within complex working environments. An enthusiastic, innovative individual who multitasks and has an excellent sense of counter strike to get results by instilling commitment, trust, fairness, and loyalty. Strengths include a strong sense of leadership, proficient communication and problem-solving skills and acts as a change catalyst. The first known individual among his compatriots to have furnished a Ph.D. (Computer Science) dissertation in ASCII Text Steganography, a research area regarded as the most difficult to comprehend by the gurus of the particular trait. Holding Master Degrees in Information Security, Project Management, and Telecommunication, he has contributed the research arena with international peer-reviewed journals and conference publications besides being the winner of the best conference paper award in Dubai's ICPINE, January 30-31, 2017.