Захист інформації в різних комунікаційних середовищах вважається істотною вимогою в сучасній технології передачі інформації. Таким чином, існує постійний пошук різних сучасних методів, які можуть використовуватися для захисту даних від зловмисників. Стеганографія – це один з тих методів, який можна використовувати для збереження авторських прав, використовуючи його для приховування зображення логотипу видавця всередині відеокадрів. В даний час більшість популярних методів відео-стеганографії стають звичайним методом для зловмисників, тому існує потреба в сучасній і продуманої стратегії захисту авторських прав на цифровому відеофайлі, коли запропонована система має на меті створити гібридну систему, яка поєднує в собі властивості криптографії та стеганографії, а також працює для захисту прихованих авторських прав даних від різних типів атак зі збереженням характеристик вихідного відео (якість і роздільна здатність). У цій статті представлений сучасний метод відео-стеганографії, що використовує переваги турбокоду для шифрування пікселів зображення логотипу та процедуру молодших двійкових розрядів для вбудовування пікселів шифрування в кадри відеофайлу. Вставка виконується в частотній області шляхом застосування швидкого перетворення Фур'є по відеокадрах. Перевірка запропонованої архітектури проводиться за допомогою індексів структурного подібності, середньоквадратичної помилки і пікового відношення сигнал/шум) шляхом порівняння вихідного і вилученого логотипу, а також вихідного і стеганографічного відео (усереднені загальні цифрові кадри в відео). Результати моделювання показують, що цей метод довів високу безпеку, надійність, пропускну здатність і забезпечує істотне підвищення продуктивності в порівнянні з існуючими відомими способами з меншими спотвореннями в якості відео

Ключові слова: відео-стеганографія, авторське право, швидке перетворення Фур'є, турбокоди, молодший двійковий розряд

UDC 004
DOI: 10.15587/1729-4061.2020.201010

DESIGN AND SIMULATION A VIDEO STEGANOGRAPHY SYSTEM BY USING FFT-TURBO CODE METHODS FOR COPYRIGHTS APPLICATION

Abbas Ali Hussein
Master Student*
E-mail: eng.abbasalsaeedi@gmail.com
Osama Qasim Jumah Al-Thahab
Professor, Doctor of Electronics and Communications Engineering*
E-mail: osamaalthahab@gmail.com
*Department of Electrical Engineering
University of Babylon
Al-Hillah, Babylon, Iraq

Received date 13.02.2020
Accepted date 20.04.2020
Published date 30.04.2020

1. Introduction

Many people when they are thinking about protecting their confidential data during transition them over various type of the communication channels, the initial word that coming to their minds is "Hacking'' and how it can be overcoming. Steganography Technique is one of the sciences that may help the people to defeat hackers by hiding the presence of the secret data (hide or embed) inside the cover medium (carrier) in ways that forbidden discover (detect) it by people who do not have the right to see it (in other words, just the sender and receiver know the presence of the secret data) [1].

"Steganography" word is coming from mixing two Greek words "Steganos" and "graphy" which meaning "covered" and "writing" Respectively. Thus, made Steganography word exactly means "covered writing". The most notable species known of the Steganography are (audio, images, video, etc.) [2, 3].

The development of the internet technologies demonstrates the possibility of using the video Steganography technique as a powerful and secure method for sharing secret data likes (banking information, medical records, military intelligence copyright, etc.) inside different internet platforms where the digital videos file has many features as compared with other Steganography types. For instance, video Steganography technique proved a low distortion in a video file after embedding data in its which can be handled faultlessly, and the hidden data are invisible to the human visual system with high capacity for embedding the data and many other features [4].

To deeper understand the "Steganography" process must first understand the "Cryptography". The Cryptography is the technique of transformer the secret message (information) into another format named "ciphertext" can't be readable by an unauthorised person. So that, it can be considered the cryptography is complementary to Steganography process. Where the secret message encrypted before hiding it in cover medium that adds a high degree of security and hardiness.

Someone can consider that the Cryptography and Steganography are cousins belongs to spy craft family. Cryptographic convert the secret data into the unintelligible (unreadable) form, while the Steganography attempt to conceal the presence of secret data by hiding it in the cover file [5].

Therefore, studies that are devoted can be used separately to solve many of problem in communication system like improved the security of the communication system to transition data, maintain the copyright of transmitted

digital file and many other features. But this proposed study is concentrated to employ the characteristics of those techniques together (Cryptography and Steganography) to build a high level and powerful security system works to maintain the copyright of digital video file from various types of attack.

2. Literature review and problem statement

There is a lot of research in the science of hiding data inside the video file (Video Steganography) where the highlights of the previous study are shown in the following part to understand their strategies involved.

The paper [6] suggests Steganography technique depended on detecting the human skin regions inside a video file and considered it as the ROI (Regions Of Interest) which used to hosting the embedding process by applying the adaptive skin detection algorithm on each video frames. Then converted the detected skin region into a skin-block-map to reduce the error-prone skin pixels. After that, the embedding (hiding) process is performed by employing a wavelet quantization technique (three-level Discrete Wavelet Transform) over the blue and red channels of the carrier frames to improve the strength of the system. However, the protection of the embedded message was not developed where the embedded in skin regions is not sufficient to protect the secret data. Therefore, this algorithm can be developed by applying cryptography on the data before hiding its algorithm, in that way, the defense of the information can be increased against the attacker.

The paper [7] suggests a secret Steganography procedure, to hide the secret data file inside the digital video file. In this method, double coding mechanism is applied by using a couple of types of coding on the same secret data one following another (pseudo-random codes and Morse codes). The system is performed in the wavelet domain by applying (2 level – Discrete Wavelet Transform) on the frames before hiding data in its. This algorithm produces a good performance and protection. The weakness of this approach is time consumption as well as small embedding capacity, which can be improved if embedding is done in least two significant bit.

The paper [8] proposes a Video Steganography algorithm to hide two digital videos file inside another video file by employing the principle of a DWT(discrete wavelet transform). Where in this method, both the cover video and the two secret videos converted into frames. After that, applying the DWT on the frames of the carrier video and turned it into four bands (Low Low "LL", High High "HH", High Low "HL", Low High "LH"). Later utilizing the principle of least significant bit technique to embed the pixels the two secret video frames inside HH, HL, LH bands of cover frames. The weakness of this approach is the low-security level which can be better if cryptography procedure is applied on the secret data before hiding it's in the video.

The paper [9] proposes an algorithm depended on a hash-based least significant bit substitution (HLSB) in the spatial domain. This Steganography technique converts the video into its frames and then split each frame into a red and green and blue frame. Later, divided every eight bits of the secret message into 3, 3, 2 segments and hide it inside the Red, Green and Blue pixel values of the digital cover frame respectively. Finally, let's rebuilt the Stego-video using all frames. Anyway, this technique can be improved if encrypted the secret message before embedding in video.

The paper [10] considers approach a digital video Steganography procedure to hidden secret message file inside the video. The method depended on BCD coding (Binary coded decimal) to encrypt the secret data. Then, implanted it inside the video. The embedding is done in wavelet domain in the middle and high frequencies zones after apply 2D – Discrete Wavelet Transform on selected video frames. The resulting frames are Stego-frames which contribute with other unchanged frames to build the output Stego-video.

The paper [11] presents a video Steganography by depending on using RSA (Rivest–Shamir–Adleman), Huffman encoding, and random DNA strand encryption to encrypt the secret data before embedding in a video frame. The system proved an excellent level of security, but the limitation in this method is low embedding capacity as well as the time consumption capacity, which makes relevant study useless. A way to overcome these difficulties can be one encryption robustness technics like turbo code as display in our algorithms.

The paper [12] proposes an efficient method to transport information by video Steganography. The system was built to secure the medical image by concealing it into a digital video where its data integrity and confidentiality can be improved. The method was utilising movable object in the target video to hide the image bits. However, these systems could be further enhanced if they thought to add the level of protection, for example, cryptography.

The paper [13] suggests a video Steganography technique to hide a secret data inside video file the frequency domain by applying Discrete Cosine Transform on video frames then embedded secret message in its. The system proved good security and good capacity to hide the data. However, the security of that algorithm can be enhanced by using secret-key or encryption technique to encode the secret data before hiding. Our proposed system solves that problem by using turbo code.

The paper [14] presents a video Steganography algorithm to hide the secret data inside a video by using Hamming codes (15, 11) to encode the data before embedding and multiple objects tracking algorithm to select the embedding position in the video. The algorithm proves an excellent security level, but embedding capacity in this method is low. However, the security needs more enhancement so it can be improved if embedding is done in the frequency domain by using suitable transform like (fast Fourier transform, Discrete Cosine Transform) as it has done in our proposed system.

The Copyright point to a collection of rights that use to save the intellectual property from theft or violation by persons is not having the permission to use this work. In the dictionary, copyright describes as "a person's exclusive right to publish, reproduce, or sell the original work". For example, republish the document, video, image, etc. Protecting these rights from attacked by hacker is an urgent necessity as a result of the growth in the attacker program which used to break those copyright.

Ago the evolution of network technology, become the legal protection of copyright a huge difficulty because of it simple and the inexpensively to copy and share a large

number of digital works as video files without with outtake an authorized right from the company the produce that digital work. So, in present-day become the violation of the copyright of the digital works by illegal piracy that made digital work infringement easier with a speedy spread to the global, that made the copyright owner is often challenging to treat by lawful means after that event [15].

Many of researchers is try to produce a ways that protect the copyright of video from infringement, but with the continuous development of piracy program that made each of previously protection techniques is a traditional and natural thing to break by the hacker. So there is a need for new smart technologies that solve the problems in previous protection algorithms with more security level and capacity [16].

The problem statement here is getting a more reliable method that not predictable as the earlier ones with more extra robustness properties against attackers with higher capacity by using the benefits of both encryptions and Steganography.

So the proposed method encrypts the pixel of the logo image (image contains authentication and ownership identification) via Turbo Code then distributed them in the Least two Significant Bit Technique of the pixels of digital video frames, so that, the mixed between secret data and cover frame will be noticeable by the Human Vision System as one piece of data.

3. The aim and objectives of the study

The aim of the study is to generate a security system used to maintain the copyright of the digital video by hiding the logo image inside the video. To achieve this aim, the following objectives are accomplished:

– generate a cryptography system used to encryption the logo image before hiding it in the video;

– generate a high embedding capacity Steganography system used to hide the encryption logo image inside the digital video file in a way that does not affect video quality and can't recognize the changing in the video file by Human Vision System (HVS);

– increase the security of the embedding technique by embedding in the frequency domain;

– generate a safety system combines between Steganography and cryptography;

– study the reliability of the system to maintain logo bits when the Stego-video transmission and received through a noisy channel, by extracting high-quality logo image from Stego-video.

4. Fundamentals of turbo code

Various types of Convolutional-Codes termed TC (Turbo-Codes) is proposed in 1993 that quickly became one of the famous and reliable models for encrypting and error correction of information bits that spread in a high-noisy channel [17]. Now, despite the passing more than two decades of TC technique but it still used in many communication systems because of the reliability and efficiency of it to encrypt bits, error correction and multiple extra features [18].

4. 1. Turbo encoder

The common construction of Turbo Code encoder is formed of at least two identical RSC (Recursive Systematic Convolutional) linked in parallel through an interleaver as presented in Fig. 1. The output codeword of that parallel connection is a systematic code consists of the combining input bits followed by the parity identical bits (redundancy bits) which result from encoding the input bits by the identical Recursive Systematic Convolutional encoders as presented in eq. (1) [19].

$$C = \begin{bmatrix} u1\, p1(1)\, p1(2), u2\, p2(1)\, p2(2), ..., \\ uk\, pk(1)\, pk(2) \end{bmatrix}, \quad (1)$$

where C represents the output code stream, u represents the input bit while p represents the parity check bits and k is a length of input data. The number of party bit that follows each input bits dependent on the number of Recursive Systematic Convolutional that connected in parallel in the turbo encoder system.

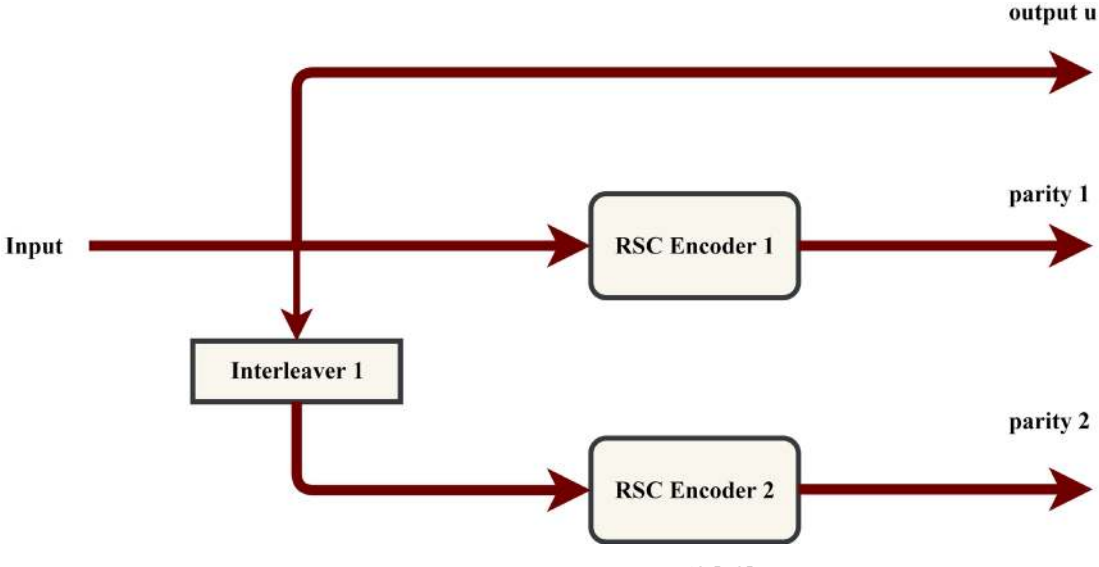

Fig. 1. Turbo encoder with rate 1/3 [19]

4. 2. Turbo code decoder

At the receiver end, the information is de-multiplexed to generate the received data vector. This signal data usually has an amount of distortion when transitioning through a noisy channel. At the receiver, the data is decoding to obtain only estimates bit of the systematic and two groups of parity bits, where the estimates provide the subsequent turbo decoder as a form of Log-Likelihood Ratios (LLR) to give the received signal. The General Structure of the TC decoder can be shown in Fig. 2.

It contains two decoding blocks combined in parallel to each other by (π) interleaver and (π') de-interleaver. The process of decoding is an iterative operation in which information called extrinsic information $Le(u_k)$ are exchange among both decoders component. Each iteration of TC is divided into two half iteration. During the first iteration half, the first encoder is enabled and work to receive the channel input (systematically encoded channel bits *Lcyks*, the check bits that sent from the associated encoder element *Lcyk*2 and the prior information $L1(u_k)$ that obtained from the opposite decoder element through de-interleaver to generate the extrinsic information data $Le1(u_k)$ as an output result. The same situation will occur at the other half of iteration where the other decoder will enable and work to receive systematically encoded channel bits after the interleave *πLcyks*, the other soft check bit *Lcyk*3 and the prior information $L2(u_k)$ will produce the extrinsic information $Le2(u_k)$. The process of iteration will remain until reached to the most desirable iteration number to achieve the wanted Bit Error Rate performance [20].

The main algorithms of turbo code are Soft Output Viterbi Algorithm (SOVA), Maximum A Posteriori (MAP) and Viterbi Algorithm (VA) which all have the same principle but with some different process. In this paper, it interests in SOVA algorithm.

SOVA is operated similar to the Viterbi decoder but with two essential modifications that let it use as a component decoder for turbo codes. First, SOVA uses a modified path metric that takes account of prior probabilities of input symbols. Second, SOVA is modified to produce a soft output that indicates the reliability of the decision. Hence, SOVA saves the survivor path metric and the path metric difference at each place where two paths merge. These path metric differences are used to produce soft-output represent a measurement of the reliability of the decision.

$L(uk\,|\,yk)$ is represented the soft output of the SOVA component decoder, and it is decomposed in three terms, as shown in eq. (2) [21, 22].

$$L(uk\,|\,yk)=Le(uk)+L(uk)+Lcyks, \tag{2}$$

$$Lc=\frac{Eb}{2\sigma 2}4\alpha, \tag{3}$$

where *Le* is extrinsic information, *Lc* is defined as the channel reliability, *Eb* is the energy/bit, σ2 is the noise variance, α is the fading for non-fading channel (*a*=1).

The inputs to the first SOVA component are:

1) *Lcyks* – the received versions of transmitted systematic bits and scaled by channel reliability;

2) *Lcyk*2 – the received versions of transmitted parity bits which produced by the first encoder and scaled by channel reliability);

3) $L1(u_k)$ –the prior information which obtained from the extrinsic information $Le(uk)$ of the second SOVA component after deinterleaving. For the first iteration the

$$L1(u_k)=0.$$

The path metrics can be calculated by the correlation to the received, as shown eq. (4).

$$M\left(S_k^s\right)=M\left(S_{k-1}^s\right)+\frac{1}{2}u_kL\left(u_k\right)+\frac{L_c}{2}\sum_{l=1}^{n}yklx_{kl}, \tag{4}$$

where $M\left(S_{k-1}^s\right)$ – the revised path metric, n the length of the message with parity, x_{kl} received the codewords.

$$Le1(uk)=L1(uk\,|\,yk)-L1(uk)-Lcyks, \tag{5}$$

$$Le2(uk)=L1(uk\,|\,yk)-L2(uk)-\pi Lcyks. \tag{6}$$

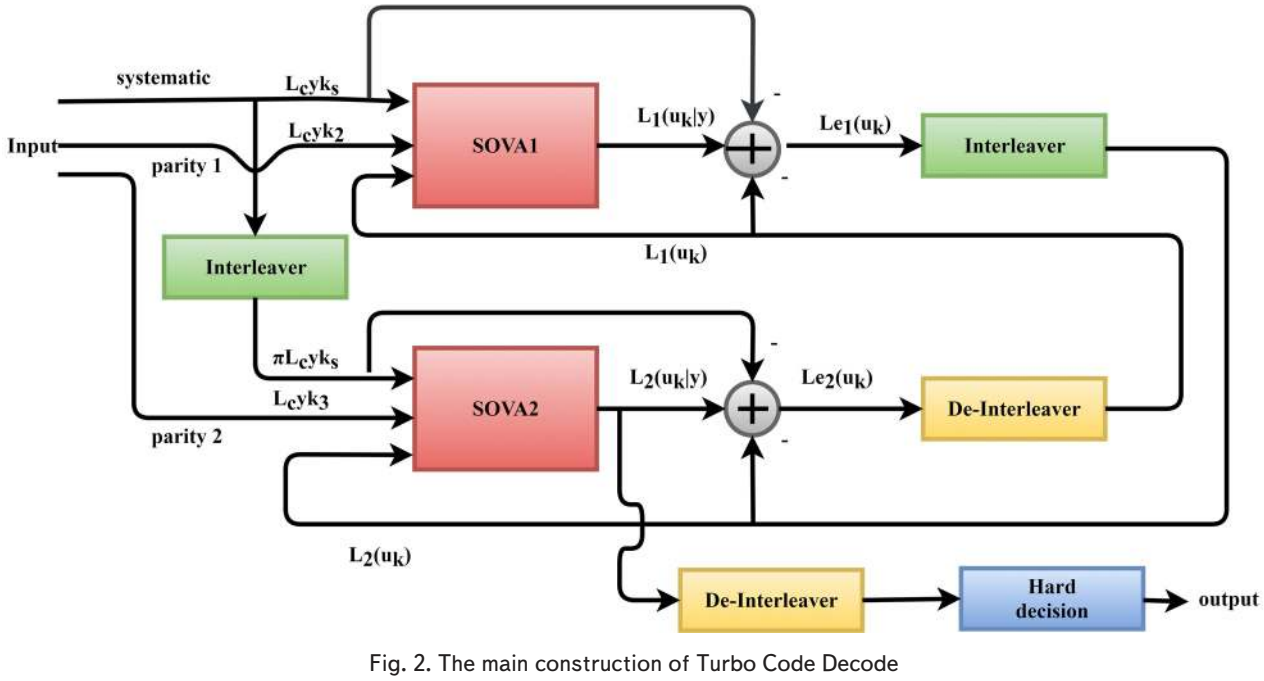

Fig. 2. The main construction of Turbo Code Decode

The is $Le2(uk)$ de-interleaved then returns to feedback as a-priori information $L2(uk)$ for the next iteration to first SOVA as priory information of the next iteration. This process is repeated in each iteration and finally stop after a specified number of iteration, whereby increasing the number of iteration better results will be achieved. At the last iteration, the soft output can be calculated from the output of the second decoder after de-interleaving and passing through the threshold detector.

5. Fast Fourier transform (FFT)

The algorithm of Fast Fourier Transform (FFT) represents the conventional method that preferred to realize a good compression performance because of reducing spatial redundancy. It is helpful in converting multi-dimensional data from the spatial domain to the frequency domain so that it is possible to perform different operations such as data compression, spread spectrum, and watermarking [23]. In digital signal processing, the transforms are widely used for processing and analyzing the discrete data and commonly used computational math. The Fast Fourier is one of that transformation which works computing the DFT (Discrete Fourier transform) and Inverse Discrete Fourier transform efficiently with a lower computational cost where that transform work to convert a signal from its original representation domain (space or time) to frequency representation and vice versa [24]. Let $f(x,y)$ be the spatial value for a matrix with size $W\times H$. The frequency domain transformation is performed by the following formula [25].

$$f(u,v)=\frac{1}{\sqrt{WH}}\sum_{x=0}^{W-1}\sum_{y=0}^{H-1}f(x,y)e^{\left(-2j\pi\left(\frac{ux}{W}+\frac{vy}{H}\right)\right)}, \quad (7)$$

where u=0 to W–1, v=0 to H–1.

Likewise, the inverse Fast Fourier transform (IFFT) is applied for computing the spatial representation domain from the frequency representation by employing the following equation.

$$f(x,y)=\frac{1}{\sqrt{WH}}\sum_{x=0}^{W-1}\sum_{y=0}^{H-1}f(u,v)e^{\left(-2j\pi\left(\frac{ux}{W}+\frac{vy}{H}\right)\right)}, \quad (8)$$

where x=0 to W–1, y=0 to H–1.

Consequently, this method can be considered as one of the most straightforward and most efficient ways for converting to and from the frequency domain.

6. Least two significant bit technique (2LSB)

2LSB one of the most advanced and straightforward techniques that use to hide (insertion) the bits of the secret data inside the digital cover frame in a way that makes the detecting of it by the natural human eyes impossible think. In this technique, each of the hidden data and each pixel of the cover frame is representing by a block of 8-bits (1-byte). The main idea of this technique is to swap the Least two Significant Bit Technique of a cover bytes by M's secret data bit. The following example explains how the Least two Significant Bit Technique operates [26, 27]. So if there is the following cover matrix and wanted to hide pixel with intensity value (210), then the following steps must be followed.

Step 1: The matrix that wants embedded data in it is;

255 3 11
180 228 129.
24 10 7

Step 2: Convert matrix from decimal to binary representation (as 8-bit);

11111111 00000011 00001011
10110100 11100100 10000001.
00011000 00001010 00000111

Step 3: Convert pixel have intensity value 210 from decimal to binary representation;

210=11010010.

Step 4: Swap the Least two Significant Bit Technique of the matrix in pixel bit data;

11111111 00000001 00001000
10110110 11100100 10000001.
00011000 00001010 00000111

Step 5: Convert the result matrix to decimal;

255 1 9
182 228 129.
24 10 7

As remarked in the previous example, 3 bytes only are altered, and the amount of change can be ignored (not have a significant effected on image quality). Therefore, the Least two Significant Bit technique system has high performance in covering data with less effect on the quality of image or video frame.

7. Proposed system

Here in this work, a modern strategy is introduced to embed a logo inside video frames by employing the benefit of Turbo system idea to encrypt logo image and least two significant bit technique to insert the logo image in the cover frames after converting the cover to the frequency domain by using Fast Fourier Transform. Fig. 3, 4 show the block diagram for the proposed method described in this article.

The following steps can be taken to perform the proposed work that described in this article:

1) convert the RGB logo image into three layers colours space (R&G&B) red, green and blue;

2) cryptography each layer in logo RGB image (Red, Green and Blue layers) by representing the logo pixels as an 8-bit binary vector. Then the bits of each pixel are encrypted by utilizing TC (turbo code) with rate 1/3;

3) convert the cover video, which wants to hide the logo image in it into frames;

4) select the frames that will embed the logo in it and convert each of them into three colours space (Red, Green and Blue);

5) apply the Fast Fourier transform on the red, blue and green colour layers. The pixels value will be converted as magnitude and the phase components as see in eq. (7);

6) embed the encrypted bits by using the insertion technique (least two significant bit) inside the frames, so that the encoded pixels of the red logo hide in a red frame and the same thing for the green and blue logo;

7) apply the Inverse Fast Fourier transform on each Red, Green and Blue layers of the selected video frames to reconstruct the components by converting them from frequency to spatial domain for producing the Stego-frame as displayed in eq. (8);

8) build the Stego RGB frame by combining the Stego red, green and blue frame as one frame;

9) lastly, reconstruct the video from the frames to get a Steganography video as seen in Fig. 3, 4.

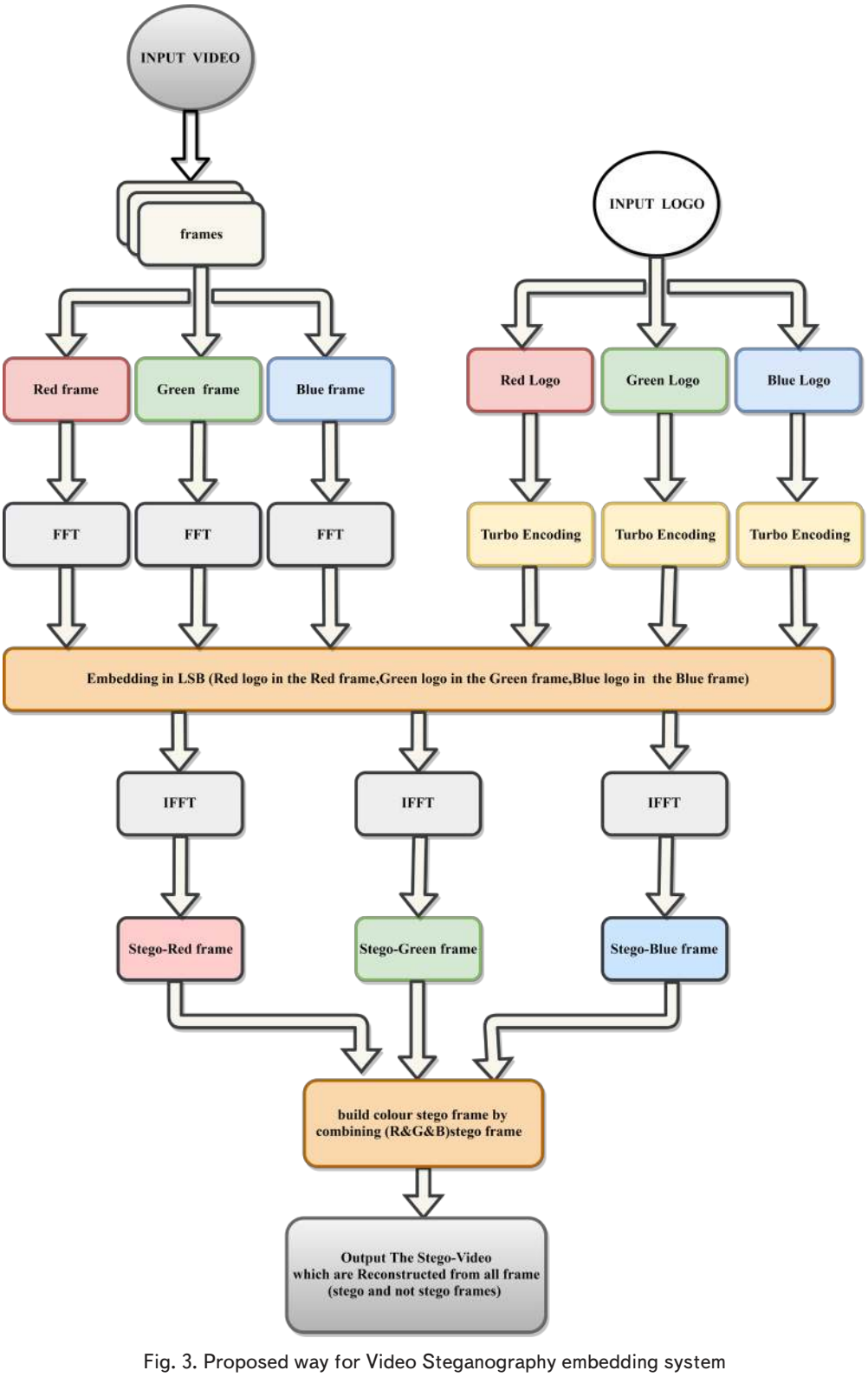

Fig. 3. Proposed way for Video Steganography embedding system

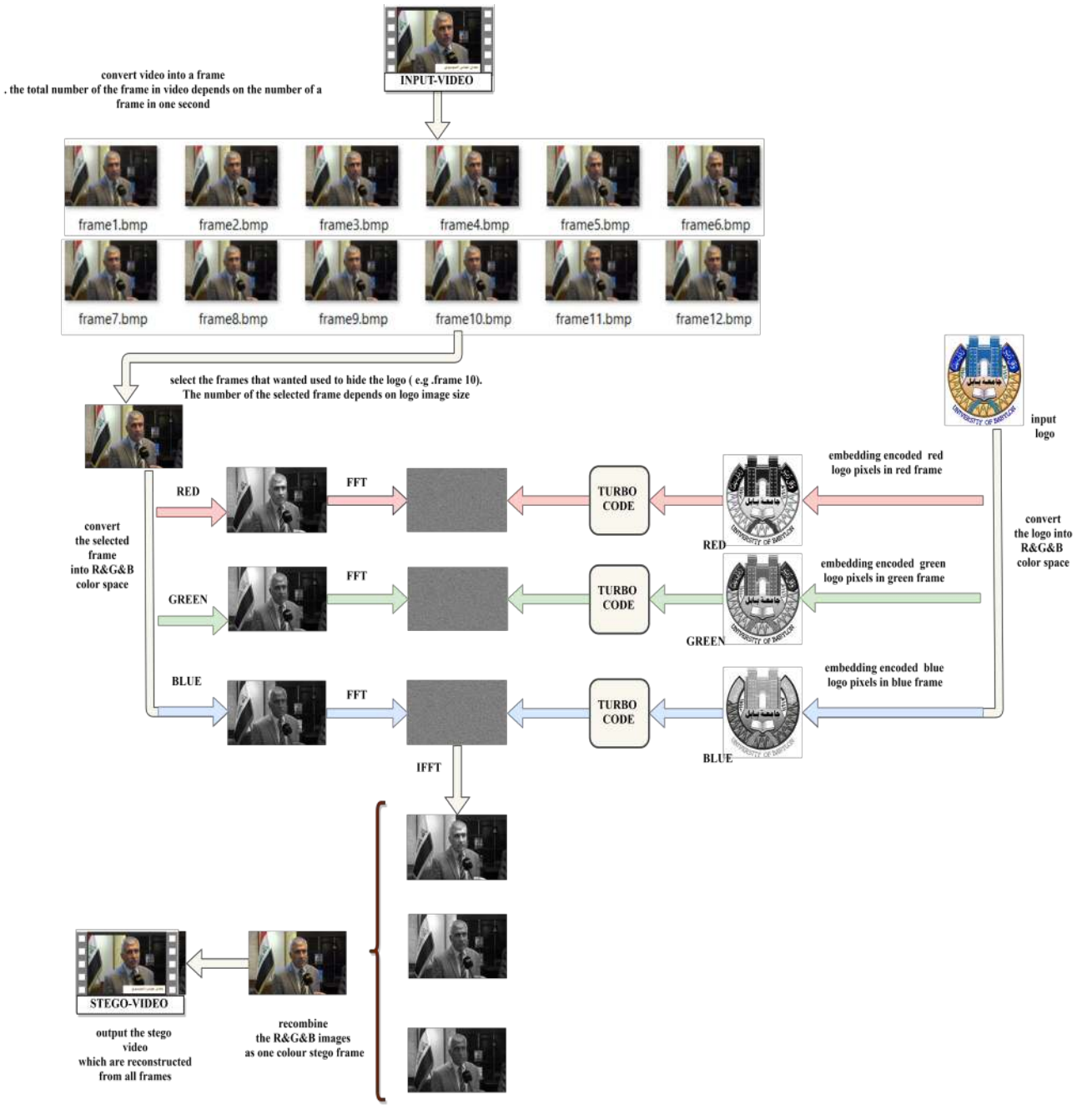

Fig. 4. Video media and embedded logo image in the proposed system

Now, After Steganography, the digital Stego-Video is available to be transported to anyone through the internet or any communication system. At the receiver end if it is necessary to extract the hidden logo image, there are some steps required as follows:

1) select the Stego-video and transformed it into frames;

2) select the frames that logo pixels hidden in it;

3) convert the selected frames into three colour space (red, green and blue). Then apply the (Fast Fourier transform) on the red, blue and green colour layer, to convert it's into frequency field (to converting it as magnitude and the phase components) as see in eq. (7);

4) extracting the red logo pixels from the red frame and green logo pixels from the green frame and blue logo pixels from the blue frame;

5) recombine the red, green and a blue logo to obtain a final colour logo. As seen in Fig. 5, 6.

The previous figures display the general procedure of the proposed system in case of embedding and extracting of the logo image. Where those figures explain the work of each technique (Fast Fourier transform, Turbo Code, Least two Significant Bit Technique) in each extracting and embedding process.

Fig. 3–6 that describe our proposed system are sketched by (draw.io) program.

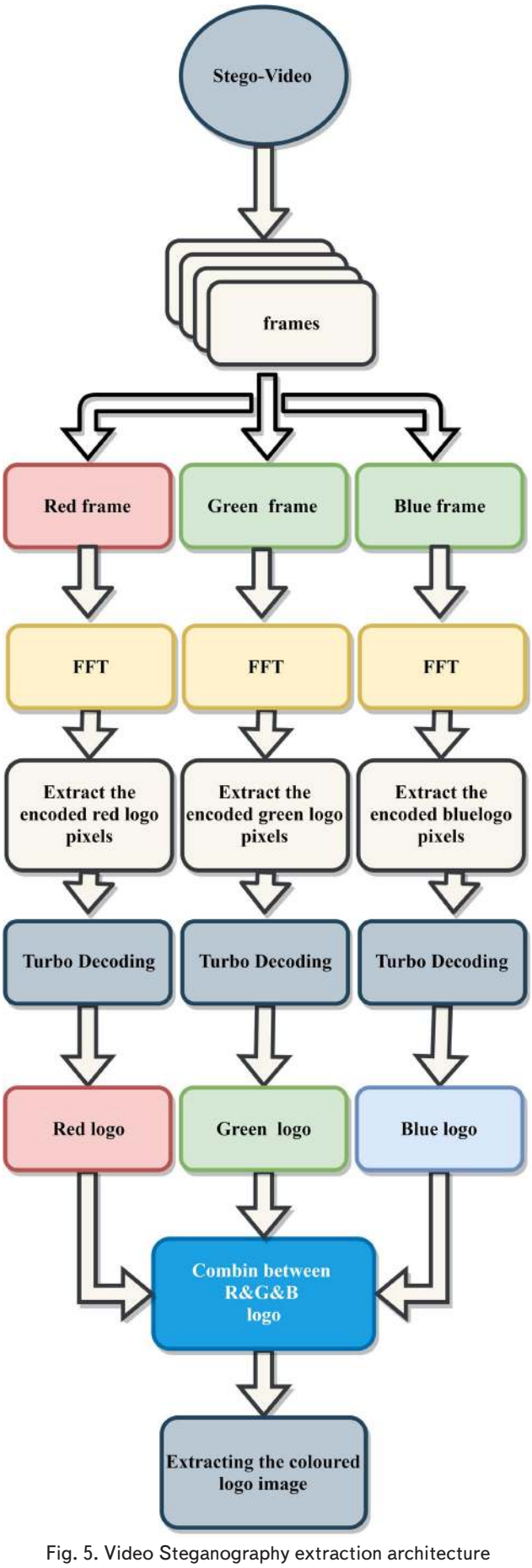

Fig. 5. Video Steganography extraction architecture

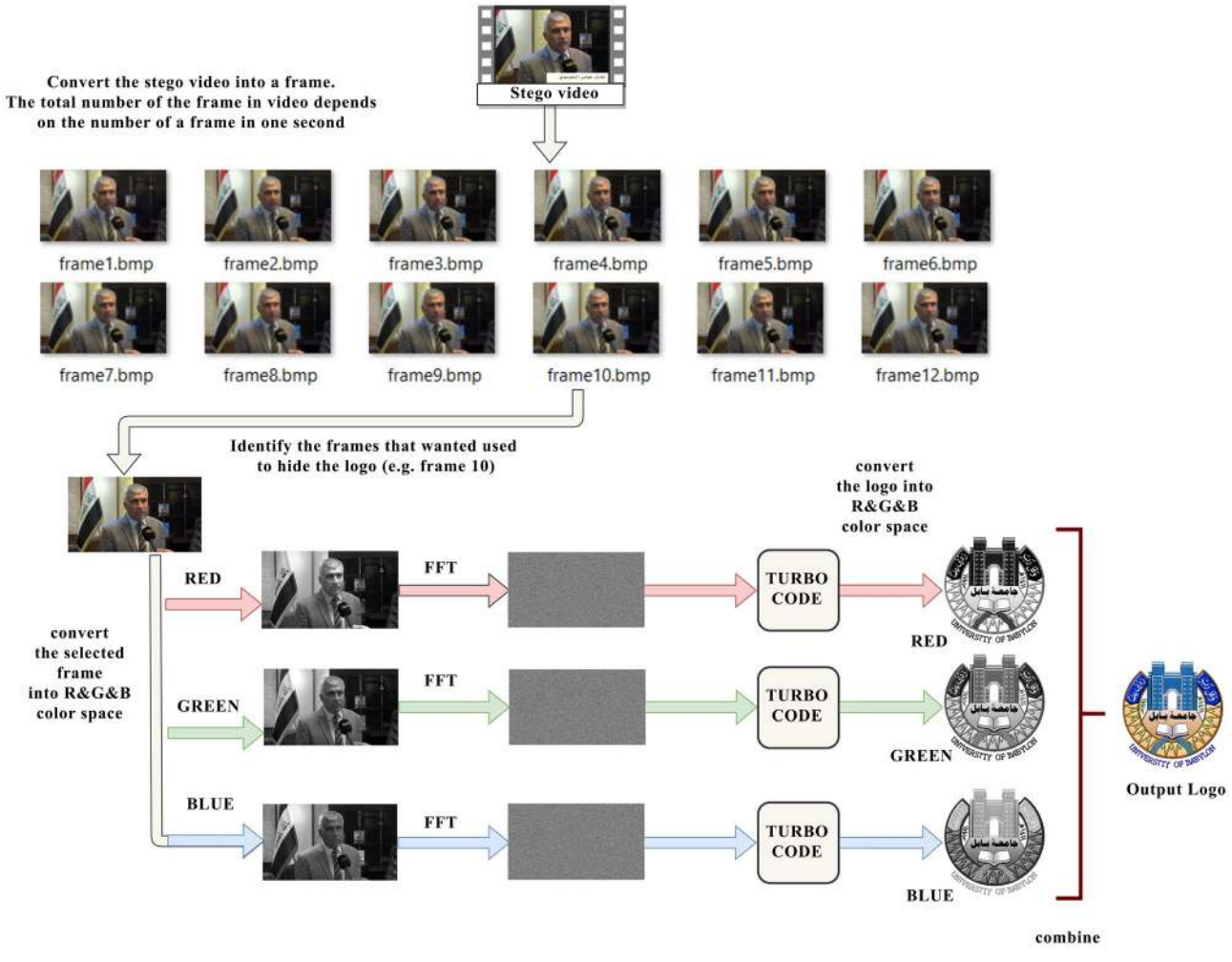

Fig. 6. Extracting the logo image from the Stego-video

8. Simulation results

The primary purpose of the Steganography strategy is hiding secret data inside the cover file in a way that can't be recognized by naked human eyes. As a result of that, the quality of the cover file will reduce, ranging from a small alteration to severe distortion. To decide whether the malformation level is acceptable or not, statistically, various tests have been employed to take the decision. There are several tests like PSNR (Peak Signal to Noise Ratio), MSE (Mean squared Error), and SSIM (Structural similarity index). The tests are applied among the frames of the original video and identical frames in the Stego-output video. MatLab 2019 performs and analyze this design.

8. 1. MSE (mean squared error)

MSE is a statistical approach that defines the identically between the frame of the original video (cover) and the frame of the Stego-video. The computation of the correspondence is doing by calculating of error signal getting from subtracting the checked signal (Stego-frame pixels) from the referred one (cover frame pixels) the equation of it can be seen in eq. (9) [28, 29]

$$MSE = \frac{\sum_{m=1}^{w}\sum_{n=1}^{h}\left[K(m,n)-K'(m,n)\right]}{w*h}, \quad (9)$$

where w, h symbol represents the video dimension, K represents the cover-video frame, $K`$ represent a Stego-video frame, m=1 to w, n=1 to h.

8. 2. PSNR Peak Signal to Noise Ratio

PSNR is a decibel scale value describes the proportion amongst the largest power of a signal and the power corrupting noise. PSNR is usually used as a standard of the quality of an image or frame where it worked to calculate the quality of Stego-frame and amount of similarity to original-frame, so the higher value of it is pointing to more top Stego-frame quality. Its equation is seen in eq. (10) [30, 31].

$$PSNR = 10\log 10\left(\frac{Higval2}{MSE}\right). \quad (10)$$

Higval is the maximum possible intensity of the pixels= =255. PSNR range between (–∞ and ∞).

8. 3. SSIM structural similarity index

Digital file processing like video, image processing is sensitive to different forms of distortions, which may occur a decline in image precision. In order to evaluate the variation in the digital video resolution and the quantity of change that may happen before and after a Steganography process. The frames that were changed after Steganography must be compared to the frames before the change. Work as an

assessment index which bases on the counting of 3-terms, namely the structural term, luminance term and the contract term The equation of Structural Similarity Index can be viewed in eq. (11) [32, 33].

$$SSIM = \frac{\left((2UxUy + T1)(2\sigma xy + T2)\right)}{(U2x + U2y + T1)(\sigma 2x + \sigma 2y + T2)}, \quad (11)$$

where, *Ux*, *Uy* represent the local means, σ*x* and σ*y* represent the standard deviations while σ*xy* represent the cross-covariance. SSIM range between (0 and 100 %).

Multiple tests were done to examine the performance of the suggested system by three well-accepted methods. Table 1 display the effectiveness of the proposed system to deal with the different size of video and logo. Table 2 presents a comparison amongst the suggested systems and another method, according to Peak Signal to Noise Ratio. Table 3 shows the quality of extracting logo in our system with and without using turbo code according to the Structural Similarity Index with different level of Salt and Pepper noise density.

Fig. 7 is a Matlab figure shows the comparison between cases if embedding is performed in the least (one, two, three, four, five, six or seven) significant bits.

As display in that Fig. 7 the impact of the increase in the number of least significant bit that uses to embedding the data on the video quality, where the quality of the frames is decreased with a notable rise in the value of Mean Squared Error with each increase in the number of using the least significant bit.

Table 1

Display the effectiveness of the proposed system

Video Resolution	Logo Resolution	Average SSIM	Average MSE	Average PSNR
240×160	196×196	99.6655	0.0872	58.9875
240×160	147×262	99.6964	0.0864	59.0292
240×426	240×427	99.7228	0.0881	58.9453
360×640	360×640	99.7046	08850	58.9260
360×640	480×480	99.6989	0.0883	58.9355
480×854	512×512	99.7924	0.0565	60.8752
480×854	854×084	99.6953	0.0884	58.9276
720×1280	720×1280	99.6914	0.0887	58.9135
720×1280	512×512	99.9036	0.0251	64.3962
720×1280	400×400	99.940	0.0153	66.535
1080×1920	720×1280	99.856	0.0394	62.427
1080×1920	512×512	99.9621	0.0110	67.950
1080×1920	400×400	99.979	0.0067	70.162
2560×1440	720×1280	99.921	0.0222	64.914
2560×1440	512×512	99.980	0.0062	70.480
2560×1440	400×400	99.987	0.0038	72.592
3840×2160	720×1280	99.965	0.0098	68.465
3840×2160	512×512	99.991	0.0028	73.953
3840×2160	400×400	99.994	0.0017	75.987

Table 2

Comparison between the Proposed System and Other Similar Systems According To PSNR

Criteria	[34]	[35]	[36]	14	10	[6]	[7]	Proposed system by FFT and 2LSB and turbo	Proposed system by FFT and 2LSB and only
PSNR in dB	52.8	54.4	29.7	54	42	51	56	68	72

Table 3

Comparison displays the benefits of using the Turbo code in our proposed system on the resolution of the logo image extracted under the effect of noise on the Stego-video

Video size	Logo size	Salt and Pepper noise density	SSIM With Turbo Code	SSIM WithoutTurbo Code
480×845	200×200	0	100	100
480×845	200×200	0.001	98.85	96.23
480×845	200×200	0.01	88.14	87.63
720×1280	300×300	0	100	100
720×1280	300×300	0.001	99.27	95.87
720×1280	300×300	0.01	86.16	84.25

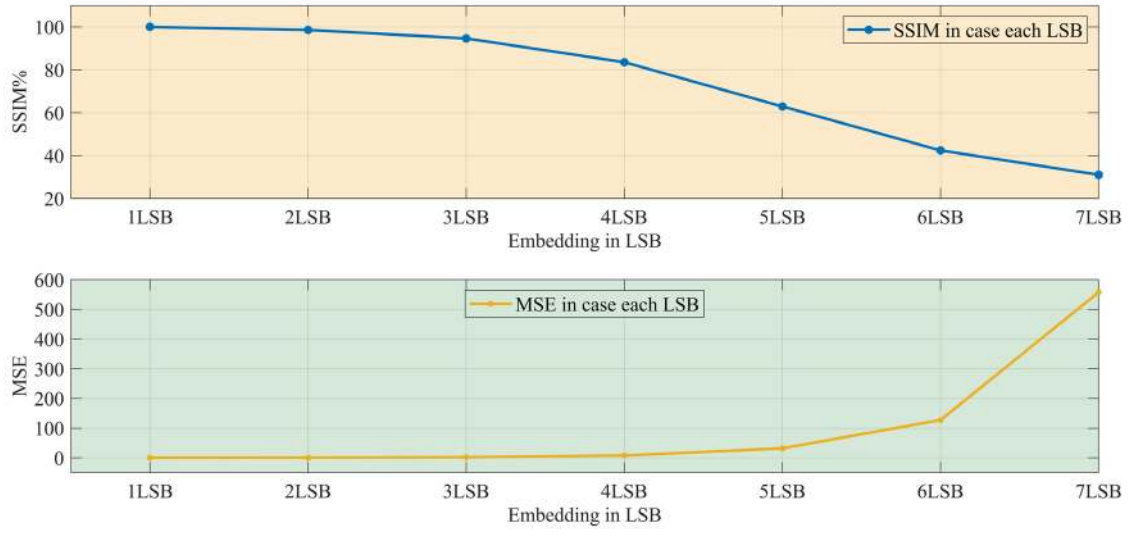

Fig. 7. Effects of using more than one least significant bit on frame quality

9. Discussion of experimental results

All previous experimental result shows that our embedding technique does not have a considerable effected on the quality of the original video after embedding data in it. Where the difference in quality between the original and Stego-video can't be noticeable. The in Table 1 there is application on the various quality of Foreman video (4K–144) after embedding different size logos it. As noted in that table the Structural Similarity is ranging between (99.6–99.99) % and the Visual Quality in dB is ranged (58.8–75.9). From all these measurements it can be concluded that the proposed system has a tiny effected of video resolution (can be neglected) with proved a high capacity to hide high-resolution logo image.

The proposed system has more efficient in quality of the video compare with the previous technique, as displayed in Table 2, which shows the average of Peak Signal to Noise Ratio of our advanced algorithm with another seven related work. It demonstrates that our procedure has higher amounts of visual quality than seven works when the same amount of data is hidden in each technique.

The results shown in the Table 3 confirm that the use of the turbo system to encrypted the logo image has another benefit besides the encrypted where it works increases the similarity (Structural Similarity) between the original hide logo with the extracted logo by reducing and correct the error bits that happen in logo after applied different levels of Salt and Pepper noise on Stego-video.

Our advanced system has many features in terms of security, video quality and capacity besides that the embedding is done in frequency, which adds another security level to this system as display in the previous experiment. Table 3 presented that is a tiny reduction in the video quality when the turbo code system used to encryption the logo bits, that reduction in video quality result from the needed to embed the parity check bits inside the video which may be effected in result Stego frame quality. That problem can be solved when used puncturing process which works to removing some parity bits from the resulting codeword in a way not effect on the security of the resulting codeword. More security level can be added to the system in the future by using another security key which works to select an embedding position in a video frame in a way close to a random embedding way.

This system work to reduce the capability to detect the secret hidden bits by an unauthorized person at a rate of 70 %. The using of turbo code work to add two check bit to each secret data bit, in this case, the probability to expect the correct secret bit by hacker is reduced to 70 % where this value is increased to reach into 100 % when using to Fast Fourier Transform to hide the data in the frequency domain where the hacker is not expected that is the data is hidden in another domain (frequency).

This result was obtained by hiding the same data in the same video with and without using a turbo code to encode the hidden data. The result shows that using the turbo code is work to increase the similarity between hidden and extracted logo at a per cent range (5–15) % when the Stego-video pass-through noisy channel.

This system work to increase the hiding capacity where embedded is done in the least two significant bit, which leads to improving the embedded capacity for video into double.

10. Conclusions

1. As of result of using the Turbo code to encrypt the logo image and convert it into unreadable data before embedding it in the video, the system has successfully to achieve a high-security encryption level. Where the using turbo code at rate 1/3 lead to reduce the ability to discover the secret hidden bits by an unauthorised person by a rate of 70 %. So it considered the second line of defense against the attack in case the ability of the attacker to break the embedding system.

2. As a result of embedding in the least two Significant Bit, the system successfully improved embedded capacity in the video into doubles. Also, the result shows that embedding in the least two Significant Bit technique has not effected on the result video quality, as shown in Fig. 7. The similarity ratio between the original video and the Stego-video (99–99.9). So it can be concluded from the results that after processing the video, the changing in the pixel values of the video frames is very tiny can't recognize by Human Visual System.

3. This system successfully achieved increasing the security from 70 % to reach into 100 % after utilising the benefits of Fast Fourier transform and Inverse Fast Fourier transform to embed in the frequency domain. Where it reduces the probability of the attacker to expect there are secret data hidden inside the video in the frequency domain.

4. By combining between Turbo code and Fast Fourier transform and least two significant bit techniques, the proposed method successfully achieved combine between Steganography and Cryptography which lead to build a powerful and high-performance technique gathering between the benefits of two systems in terms of high secrecy and concealment of information.as was shown in Fig. 3–6.

5. The system succeeds maintaining of logo image when the Stego-video transmission and received through a noisy channel where the turbo code has another advance as shown in Table 3 where it works through decoding to estimate an actual value and correct the errors bit that may result by noisy channel.

References

1. Sadek, M. M., Khalifa, A. S., Mostafa, M. G. M. (2014). Video steganography: a comprehensive review. Multimedia Tools and Applications, 74 (17), 7063–7094. doi: https://doi.org/10.1007/s11042-014-1952-z
2. Selvigrija, P., Ramya, E. (2015). Dual steganography for hiding text in video by linked list method. 2015 IEEE International Conference on Engineering and Technology (ICETECH). doi: https://doi.org/10.1109/icetech.2015.7275018
3. Tyagi, V. (2012). Image steganography using least significant bit with cryptography. Journal of global research in computer science, 3 (3), 53–55.
4. Ramalingam, M., Isa, N. A. M. (2016). A data-hiding technique using scene-change detection for video steganography. Computers & Electrical Engineering, 54, 423–434. doi: https://doi.org/10.1016/j.compeleceng.2015.10.005
5. Rahna, E., Govindan, V. K. (2013). A Novel Technique for Secure, Lossless Steganography with Unlimited Payload. International Journal of Future Computer and Communication, 2 (6), 638–641. doi: https://doi.org/10.7763/ijfcc.2013.v2.243
6. Sadek, M. M., Khalifa, A. S., Mostafa, M. G. M. (2016). Robust video steganography algorithm using adaptive skin-tone detection. Multimedia Tools and Applications, 76 (2), 3065–3085. doi: https://doi.org/10.1007/s11042-015-3170-8
7. Shakeela, S., Arulmozhivarman, P., Chudiwal, R., Pal, S. (2016). Double coding mechanism for robust audio data hiding in videos. 2016 IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT). doi: https://doi.org/10.1109/rteict.2016.7807979
8. Sushmitha, M. C., Suresh, H. N., Manikandan, J. (2017). An approach towards novel video steganography for consumer electronics. 2017 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia). doi: https://doi.org/10.1109/icce-asia.2017.8307831
9. Fan, M., Liu, P., Wang, H., Sun, X. (2016). Cross correlation feature mining for steganalysis of hash based least significant bit substitution video steganography. Telecommunication Systems, 63 (4), 523–529. doi: https://doi.org/10.1007/s11235-016-0139-5
10. Rana, S., Bhogal, R. K. (2018). A Highly Secure Video Steganography Inside DWT Domain Hinged on BCD Codes. Intelligent Communication, Control and Devices, 719–729. doi: https://doi.org/10.1007/978-981-10-5903-2_74
11. Mumthas, S., Lijiya, A. (2017). Transform Domain Video Steganography Using RSA, Random DNA Encryption and Huffman Encoding. Procedia Computer Science, 115, 660–666. doi: https://doi.org/10.1016/j.procs.2017.09.152
12. Balu, S., Babu, C. N. K., Amudha, K. (2018). Secure and efficient data transmission by video steganography in medical imaging system. Cluster Computing, 22 (S2), 4057–4063. doi: https://doi.org/10.1007/s10586-018-2639-4
13. Ononiwu R., Okengwu, U. (2020). Efficient Steganography on Video File using Discrete Cosine Transform Method (DCTM). International Journal of Computer Applications, 176 (11), 22–28. doi: https://doi.org/10.5120/ijca2020920051
14. Mstafa, R. J., Elleithy, K. M. (2015). A New Video Steganography Algorithm Based on the Multiple Object Tracking and Hamming Codes. 2015 IEEE 14th International Conference on Machine Learning and Applications (ICMLA). doi: https://doi.org/10.1109/icmla.2015.117
15. Ai, L. (2015). Research on Legal Issue of Copyright Protection in the Internet. Proceedings of the 2015 International Conference on Economy, Management and Education Technology. doi: https://doi.org/10.2991/icemet-15.2015.54
16. Manaf, A. A., Boroujerdizade, A., Mousavi, S. M. (2016). Collusion-resistant digital video watermarking for copyright protection application. International Journal of Applied Engineering Research, 11 (5), 3484–3495. Available at: https://www.scopus.com/record/display.uri?eid=2-s2.0-84964047806&origin=inward&txGid=2d524ac0ac11dc78432a3692b06ab74a
17. Barbier, J., Filiol, E. (2009). Overview of Turbo-Code Reconstruction Techniques. IACR Cryptology ePrint Archive. Available at: https://eprint.iacr.org/2009/068.pdf
18. Shaheen, F., Butt, M. F. U., Agha, S., Ng, S. X., Maunder, R. G. (2019). Performance Analysis of High Throughput MAP Decoder for Turbo Codes and Self Concatenated Convolutional Codes. IEEE Access, 7, 138079–138093. doi: https://doi.org/10.1109/access.2019.2942152
19. Xu, S., Liu, B., Zhang, L., Xin, X., Rahat, Rao, L. et. al. (2017). Low complexity turbo matching coded optical transmission system based on code weight decision. 2017 16th International Conference on Optical Communications and Networks (ICOCN). doi: https://doi.org/10.1109/icocn.2017.8121491
20. Moon, T. K. (2005). Error correction coding: mathematical methods and algorithms. John Wiley & Sons, 800. doi: https://doi.org/10.1002/0471739219

21. Abrantes, S. A. (2004). From BCJR to turbo decoding: MAP algorithms made easier. Faculdade de Engenharia da Universidade do Porto (FEUP). Available at: https://repositorio-aberto.up.pt/bitstream/10216/19735/2/41921.pdf
22. Le, V. H. S., Abdel Nour, C., Boutillon, E., Douillard, C. (2020). Revisiting the Max-Log-Map Algorithm With SOVA Update Rules: New Simplifications for High-Radix SISO Decoders. IEEE Transactions on Communications, 68 (4), 1991–2004. doi: https://doi.org/10.1109/tcomm.2020.2966723
23. Al-Thahab, O. Q. J. (2016). Speech recognition based Radon-Discrete Cosine Transforms by Delta Neural Network learning rule. 2016 International Symposium on Fundamentals of Electrical Engineering (ISFEE). doi: https://doi.org/10.1109/isfee.2016.7803208
24. Nugraha, R. M. (2011). Implementation of Direct Sequence Spread Spectrum steganography on audio data. Proceedings of the 2011 International Conference on Electrical Engineering and Informatics. doi: https://doi.org/10.1109/iceei.2011.6021662
25. Shaukat, A., Chaurasia, M., Sanyal, G. (2016). A novel image steganographic technique using fast fourier transform. 2016 International Conference on Recent Trends in Information Technology (ICRTIT). doi: https://doi.org/10.1109/icrtit.2016.7569519
26. Al-thahab, O., Hassan, H. (2019). RGB Image Watermarking System based on Cubic Spline Controller Key for Copyright Applications. Jour of Adv Research in Dynamical & Control Systems, 11 (01), 1896–1905.
27. Shinde, P., Rehman, D. T. (2015). A Survey: Video Steganography Techniques. International Journal of Engineering Research and General Science, 3 (3), 1457–1464.
28. Deshmukh, P., Rahangdale, B. (2014). Data Hiding using Video Steganography. International Journal of Engineering Research & Technology, 3 (4), 856–860.
29. Paul, R., Acharya, A. K., Batham, S., Yadav, V. K. (2013). Hiding large amount of data using a new approach of video steganography. Confluence 2013: The Next Generation Information Technology Summit (4th International Conference). doi: https://doi.org/10.1049/cp.2013.2338
30. Hanafy, A. A., Salama, G. I., Mohasseb, Y. Z. (2008). A secure covert communication model based on video steganography. MILCOM 2008 - 2008 IEEE Military Communications Conference. doi: https://doi.org/10.1109/milcom.2008.4753107
31. Naji, S. A., Mohaisen, H. N., Alsaffar, Q. S., Jalab, H. A. (2020). Automatic region selection method to enhance image-based steganography. Periodicals of Engineering and Natural Sciences, 8 (1), 67–78. doi: http://dx.doi.org/10.21533/pen.v8i1.1092
32. Wang, Z., Bovik, A. C., Sheikh, H. R., Simoncelli, E. P. (2004). Image Quality Assessment: From Error Visibility to Structural Similarity. IEEE Transactions on Image Processing, 13 (4), 600–612. doi: https://doi.org/10.1109/tip.2003.819861
33. Mohammed Ali, S. I., Ghazi Ali, M., Abd Zaid Qudr, L. (2019). PDA: A Private Domains Approach for Improved MSB Steganography Image. Periodicals of Engineering and Natural Sciences (PEN), 7 (3), 1405–1411. doi: https://doi.org/10.21533/pen.v7i3.776
34. Mstafa, R. J., Elleithy, K. M. (2014). A highly secure video steganography using Hamming code (7, 4). IEEE Long Island Systems, Applications and Technology (LISAT) Conference 2014. doi: https://doi.org/10.1109/lisat.2014.6845191
35. Hashemzadeh, M. (2018). Hiding information in videos using motion clues of feature points. Computers & Electrical Engineering, 68, 14–25. doi: https://doi.org/10.1016/j.compeleceng.2018.03.046
36. Hu, S. D. (2011). A Novel Video Steganography Based on Non-uniform Rectangular Partition. 2011 14th IEEE International Conference on Computational Science and Engineering. doi: https://doi.org/10.1109/cse.2011.24