A Novel Blind Digital Watermarking Technique for Stegano-Encrypting Information Using Nine-AC-Coefficient Prediction Algorithm with an Innovative Security Strategy

CHADY EL MOUCARY
Department of Electrical, Computer and Communication Engineering
Notre Dame University-Louaize
P.O. Box 87 Tripoli, Barsa, El Koura
LEBANON
celmoucary@ndu.edu.lb http://www.ndu.edu.lb

BACHAR EL HASSAN
Laboratory of Electronic Systems, Telecommunications, and Networking (LASTRE)
Lebanese University
Faculty of Engineering I, Al Arz Street, El Kobbeh, Tripoli
LEBANON
bachar_elhassan@ul.edu.lb http://www.ul.edu.lb

Abstract: This paper presents a new methodology for data hiding using digital watermarking in the DCT Domain. The methodology relies on a new scheme for encrypting the data prior to the embedding stage. The key used for ciphering is almost of arbitrary length, type and format; this endows the watermark with a powerful, 3-level reinforced security structure. It is a blind-detector watermarking technique and the amount of the hidden data is increased by 60% compared with the traditional AC-Coefficients Prediction algorithm while sustaining a high level of transparency. Simulation results were carried out which demonstrated a promising PSNR, limited blocking artifacts, and a satisfactory level of the overall performance. The paper also presents an extensive survey of prominent digital-watermarking research outcomes in the WSEAS Transactions.

Key-Words: Steganography, Encryption, Signal Scrambling, Increased Insertion Capacity, Digital Watermarking, Discrete Cosine Transform Domain, AC Coefficients Prediction

1 Introduction

With the brisk evolution in e-Technology, Digital Watermarking has been presented and approved as a proficient resolution for the safekeeping of digital assets exposed and/or trafficked over the Internet. Digital Watermarking has grown ever since and expanded to encompass other crucial and diversified applications, which mostly fall under the umbrella of data hiding in its general gist.

Data hiding is the science of concealing information (a secret message) for a specific purpose and, History, since ancient eras is rich with instances where people have benefited from it for different intents: As far as the 5th Century B.C., Histiaeus tattooed the shaved head of his herald to convey a message (covered by the grown hair) to Aristagoras, against the king of Persia; Mary Queen of Scots hid letters in the bunghole of a beer barrel to convey messages outside of her prison; more recently, steganography was employed during World War II where Nazis used Microdots to squeeze several pages of information [44].

Data hiding has grown ever since and utterly transformed; while it originated as an instinctive art, it now became a well-defined science with its own resourceful schemes. To name a few amongst its innumerable applications, data hiding is employed in medical [8][12][27], military [23], national security [48], forensics [47][48], fingerprinting [2], broadcast monitoring [14], copyright authentication [22][29], land consolidation [30], individuals, etc. Nonetheless, there is still an overlooked perplexity when watermarking is mentioned with steganography and cryptography. Actually these labels or tags are closely interrelated and constitute a multifaceted core.

While Cryptography aims at camouflaging the undisclosed message by working on the visual layout or appearance of the *host* (the means for conveying the secret information), Steganography carries out obscuring its existence within the *intrinsic attributes* of the host using technically a more advanced and computerized modus operandi. When these two disciplines are jointly harnessed, they engender a potent means to secure conveying data.

Watermarking was originally the art of stamping a product with a visible watermark or logo to hinder counterfeiting and for ownership identification [23]. When watermarking bifurcated into the need of inserting *invisible* watermarks (*transparent signature*), it became a powerful tool for steganography, the relevant science of concealing information. In this sense, steganography aims at instilling a *protracted* invisible watermark using watermarking techniques. Consequently, one can state that watermarking is dedicated for a long-term use whereas steganography is dedicated for short-term use. Indeed, steganography tackles conveying more-developed information in a confidential manner, which is to be acted upon almost immediately by the receiver whereas watermarking per se instills information that could be used years after (no expiration date) to indubitably elucidate disputes pertaining to ownership. In this sense, the main difference between steganography and watermarking is the application and not actually the science behind.

When steganography is applied in watermarking with exercise of cryptography, the outcome is a versatile protocol that offers more than simply a double-layered information-hiding scheme; indeed, it renders almost impossible the detection, deciphering, and/or eradication of the hidden information. The use of a stego-key as “password” endows the overall function with a high-level of privacy and security. Suspicion is the first “enemy” of cryptography; ciphering the information often attracts malicious intruders, and “*steganoing*” solely, demonstrated to be insufficient as the ongoing advancement of computer software makes it feasible for expert hackers to locate the watermark and eventually decode it or eliminate it [46][47]. This could be of calamitous repercussions especially when dealing with military, medical, or other sensitively-private applications. Let’s agree that the amalgamation of these three sciences promotes data hiding to the stand of a reliable “*shield*” and puts the hidden information on a conspicuous caliber on the protection scale.

This paper will be divided into the following sections: first we will formulate the problem and tackle the choice of a suitable watermarking technique from a general viewpoint; we will also review the synopsis of cryptography and steganography (Section 2). Afterwards, an extensive survey of prominent researches fathered by WSEAS Transactions will be presented (Section 3). In the following section (Section 4), the algorithm for blind watermarking in the DCT domain using nine AC coefficients prediction will be presented and discussed; also the use of the key for encrypting and scrambling the message prior to insertion will be developed. Finally, Section 5 is dedicated to simulation results where we will demonstrate the performance of the proposed method and Section 6 summarizes the presented work.

2 Problem Formulation and Criteria for a Suitable Solution

Digital watermarking can be classified from much diversified perspectives [18][28].

2.1 Casting Method

Based on the casting method there exist two categories of watermarking: intensity in the ***spatial domain*** such as: the well-known LSB substitution technique [4][6][26], Code Division Multi Access (CDMA) [49], Spread-Spectrum [28][31][39], etc. and the transform-coefficients’ magnitude in a ***transform domain*** such as: Discrete Cosine Transform (DCT) [17][25], Discrete Wavelet Transform (DWT) [10][30][31], Fast Fourier Transform, Hadamard Transform [19], Haar Wavelet [7], Hough Codes [24], Neural Networks [7], Singular Value Decomposition (SVD) [1], BCD Codes [9], Multiwavelet [11], and other mathematical operations [24][26][28]. While spatial domain offers a high capacity of integration and allows for easily-implemented procedures, the main goal behind watermarking in a transformed domain is to deter attackers from decoding the watermark since the image is not directly altered as for the pixels domain.

2.2 Performance Attributes

Each of the aforementioned methodologies has its pros and cons depending on a criterion to optimize. Criteria for a suitable algorithm depend mainly on three major attributes: Robustness, Transparency and Capacity. These attributes are not independent from each other, rather they are closely interrelated.

Robustness refers to the possibility of an interloper to locate, decode, and/or abolish the watermark. Robustness in general can be subdivided into two essential subcategories, benign and malign attacks [29]. Benign attacks are unintentional and usually caused by diverse signal-processing manipulations such as compression, noise, filtering, and geometric distortions such as rotation, scaling, cropping, [13][24] etc. whereas malign attacks are usually performed by expert hackers with the intention to tamper the host image for a specific purpose.

Transparency pertains to the fact that the cover image or host in general, is not perceptually affected by the implantation of the watermark whether it was achieved via addition or substitution of bits, i.e., embedding the watermark would not cause the HVS [10] to detect any suspicious abnormalities in the final product. The aforementioned techniques differ from each other in the way they amend the host when embedding the watermark, i.e. luminosity, boundaries/edges, brightness/texture, layers, coefficients, etc. [25]

Capacity, sometimes referred to as *data payload*, refers to the size of the message that could be *fastened* to the host. Watermarking assets, for mere ownership certification and copyright protection uses small-sized watermarks since it is usually a logo or a simple text that undoubtedly reveals the original holder or possessor. On the other hand, when steganography is applied in watermarking, the size of the watermark could be much bigger since the watermark constitutes a more elaborate message or information for covert communication.

Watermarking techniques compete to achieve the best of these three crucial criteria. Nevertheless, it is often problematic because these criteria are somewhat complementary and improving one would cause the two others to worsen. Usually, a compromise is to be found and a priority scale is fashioned where one criterion prevails according to the application's intent (see Fig. 1).

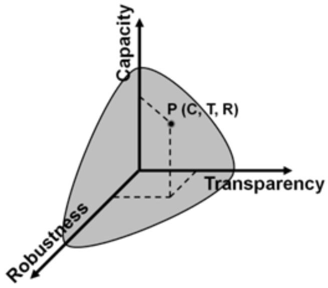


Fig. 1 – The Perplexing Dilemma

Also the complexity or ***computational cost*** of the overall process is to be taken into account when opting for or evaluating a watermarking method [3].

2.3 Fragile and Semi-Fragile Watermarks

Digital watermarking has also evolved into what is called the *fragile* and *semi-fragile* classes. ***Fragile*** watermarks are highly sensitive to any tampering attempt [27] whether benign or malign and the attacked image can, reliably and most-probably *report* this attempt. Consequently, this class of watermarking reveals to be promising in the field of image and video authentication [31]. On the other hand, fragile watermarking fails when it is about real-time applications where images commonly undergo unintentional alterations. Consequently, ***semi-fragile*** watermarks are a good concession for applications where malicious attacks are to be revealed and important features for a good semi-fragile watermark could be found in [3].

2.4 Need for Data at the Extraction Stage

Another important classification of Watermarking pertains to the need for the host image and/or the key at the watermark extraction stage (receiver end). We say that watermarking is ***non-blind*** when the extraction of the watermark requires the use of both the original image and the key used for embedding; a watermarking is said to be ***semi-blind*** when it requires the presence of only the watermark in addition to the secret key whereas a ***blind*** watermarking [10] scheme does only need the secret key for retrieval.

2.5 Key Features

The *key* for concealing the data in the cover is of prime importance and there exists two different configurations. In a ***symmetric-key*** configuration, the same key is used for encryption and decryption and quickly the key management problem drastically escalates for the number of keys increases as the square of the number of network members [16][23]. This dilemma created a crucial practical hindrance for cryptographers. In 1976, W. Diffie and M. Hellman [41] shook the entire world of cryptography by inventing the notion of public key, which is now known as the ***asymmetric-key*** cryptography. In this configuration, a *private key* and a *public key* are used; although interrelated, one is computationally unattainable from the other. It made the creation of a key unproblematic, yet difficult to falsify. Public-key algorithms are most often based on the computational complexity; the complexity of RSA is related to the integer factorization problem, while Diffie-Hellman and DSA are related to the discrete logarithm problem [42]. More recently, elliptic curve cryptography has developed in which security is based on number theoretic problems involving elliptic curves [3].

2.6 Innovative Approach for Key Generation

In this paper, the approach for key generation is fundamentally different; it relies on the idea that a logical combination or sequencing of binary numbers, no matter how astutely generated it is, will always be reminiscent and somehow feasible to decode or "decipher" especially with the aid of more and more "intelligent" computer software and the increase of computational capacity of nowadays sophisticated processors. Thus, we will employ a sort of randomly generated keys that do not exhibit any kind of mathematical or logical interrelation; the key for ciphering/deciphering will be picked almost arbitrarily and will represent anything that the users would like to adopt. The only condition is that this key could be numerically handled by a computer. Practically speaking, this constitutes an innumerable source for key generation, thus offering a somewhat reasonable solution for key handling. Additionally, it offers an almost indestructible oyster to conceal the key since any expert hacker would be misled while tackling the hidden information. Even if a suspicious interceptor or trespasser know about the existence of a hidden message or watermark, its eradication or retrieval would be extremely demanding and costly; the watermark would be practically rendered impregnable.

There exists a broad collection of cryptanalytic attacks; they are usually delineated relying on what an attacker knows and what resources are on hand. C. Shannon and W. Weaver ascertain that if one uses a key that is of strictly random substance and of equal or greater length than the hidden information, that key is strictly unbreakable provided that it is not reused in any other cryptographic material [43]. This is another motive that sustains our approach; the length of the key is highly versatile and could be chosen to be of equal length of the message to be hidden depending, of course, on the size of the host image. This factual result endows our approach with much maneuvering margins in the choice of the overall watermarking structure. This property, added to the randomness of the choice would entitle the watermark with a superlative degree of security and the virtue of a user-friendly interface.

The key could be chosen from any source of practically any type; the key could be a simple text or even a non-logical concatenation of alphabetical characters belonging to any or different languages, an image, or a cropped section of an image. The key could also be a part of an audio file that could represent a song, a registered voice, or a section of any musical material. The only condition is that these materials would be transferrable to a binary sequence, which is feasible for all the above-listed sources. This is an open source in the sense there are no limits or restrictions on the key. Moreover, none of the aforementioned sources contains inherent logical or mathematical correlation or function that could fit into a standard deciphering algorithm.

2.7 Choice of the DCT Domain

The most frequently used technique for image compression is JPEG [8] and it is inevitable for web bandwidth limitation. Since 1998, JPEG compression has been implemented using a Discrete-Cosine-Transform (DCT) coding scheme of the image which naturally lends itself to a robustness platform for data hiding when compared to the spatial domain. In fact, DCT takes advantages of redundancies in the data by grouping pixels with similar frequencies together. If lossy compression is acceptable, each data unit can then be processed through Quantization Tables [11] which yield half of the raw image discarded [38]. This approach takes advantage of the fact that the human eye is more sensitive to luminance than to chrominance.

Additionally, when compared to the Fourier Transform, DCT achieves more benefits regarding the image application: the energy compaction performance is nearly optimal and closest to KLT (Karhunen-Loeve Transform) and, from a mathematical viewpoint DCT is a reversible linear transform having real-number coefficients and provides a set of orthogonal basis functions.

For all the aforementioned reasons, watermarking in the DCT domain is very attractive and beneficial [39] [40]. Many researches and algorithms have been conducted in this domain. Gonzalez et al. [32] describes the technique which predicts a few low frequency AC coefficients for DCT and in [33] watermarking is achieved based on the modification of these coefficients. In [34] and [35], the authors present an interesting approach to increase security of the hidden data by scrambling the watermark prior to insertion using Arnold Transform. In [45] and [36], the authors implant the watermark using linear programming and adaptively weighed DC values to reduce blocking artifacts and augment the PSNR; whereas in [15] the watermarking is achieved using an Integer DCT thus enhancing the imperceptibility and watermark capacity. The insertion capacity is also increased in [37] by working on 4x4 blocks in the DCT domain.

Our proposed algorithm takes advantage of the benefits outlined by the aforementioned strategies and offers a novel implementation of digital watermarking in the DCT domain by realizing a higher capacity of insertion (60% increase), blind extraction of the watermark, acceptable PSNR and blocking artifacts, and encryption of the watermark, thus ensuring a total imperceptibility which lends itself to many applications where security is a must.

3 Survey of Related Work in the WSEAS Transactions

In [1] the authors present an asymmetric non-blind watermarking approach incorporating a secure protocol that resolves buyer/owner quarrels by generating unquestionably unique references for identification and copyright infringements. Using DCT-SVD and public key encryption with hash values, the algorithm offers a way to prevent the owner from reusing the buyer's references when dealing with other customers. The idea is to refer to Certification and Registration Authorities that'll help settle issues concerning multiple ownership claims. The approach suggests a means to trace illegal copies by generating a unique transaction identity watermark, while maintaining a higher degree of robustness for the ownership identity watermark. It also proposes a good transaction identity protocol and a copyright infringement protocol when dealing with multiple transactions of digital assets.

The authors in [2] address the issue of carrying out an inherently collusion-attack resistant scheme for hiding a logo-based watermark in *JPEG* images. They propose a protocol that averages low- and middle- frequency coefficients of DCT blocks of the image for such applications as fingerprinting where the main objective is to track the identity of illegal redistributors by reference to client-customized watermarks. Collusion attack is achieved when expert hackers scrutinize jointly different watermarking stamps belonging to one digital asset in order to surmise the technique behind it, thus allowing them to obliterate the watermark. The authors reveal an interesting Policy Generator Algorithm that allows for approximately 7315 instances of the same JPEG image to be distinctly watermarked, thus guarantying the ICAR trait. In the *US Patent 7058812* (June 2006), the holders claim the implementation of a technology that facilitates rights enforcement of digital goods using watermarks: "… If a digital pirate breaks one client and enables this client to avoid watermark detection, all content (both marked/protected an unmarked/free) can be played as unmarked only on that particular client. However, to enable other clients to play content as unmarked, the digital pirate needs to collude the extracted detection keys from many clients in order to create content that can evade watermark detection on all clients… However, in this scenario each member of the malicious coalition leaves a fingerprint in every digital good from which the estimated watermark is subtracted. Thus, like a burglar without gloves, the digital pirate leaves her fingerprints only when she commits a crime…"

We can find in [3] a content-based effective semi-fragile watermarking scheme for image authentication and content verification carried out in the DCT domain. Their approach is robust against JPEG compression and only authenticates the perceptual information in an image, yielding a good compromise between computational cost and complexity from one side and security and efficiency from the other side. The watermark is a digital signature of the visual content of the image which represents the essence carried by the low-frequency DCT coefficients and thus, authenticating the particular number of low frequency coefficient, it achieves the integrity of the image. However, if the attacker can modify the visual content without harming the watermark, the method fails. Besides, the method is vulnerable against other visual alterations such as cropping, replacing, etc. They also show that 60% to 70% of the image content can be transmitted through only the DC coefficients and the first two AC coefficients; nonetheless, the capacity of hiding data will decrease significantly. The scheme proposed is used rather for authenticating than for information hiding.

L. Y. Por *et al.* [4] present a platform that uses jointly three LSB-based watermarking algorithms to achieve steganography applied to GIF images as a medium to convey stealthy messages. The overall scheme appears as a more comprehensive tool with much versatility in configuring the outcome and endows the watermark with a high level of security via PKI mechanisms at both sender and receiver ends. It also presents a graphical user interface with integrated navigation tools. The advantage of this approach is that it enhances the traditional LSB-substitution method for RGB images and overcomes the color-palette problem by using a color cycle algorithm whereby watermarking will not significantly alter the visual characteristics of the host GIF image.

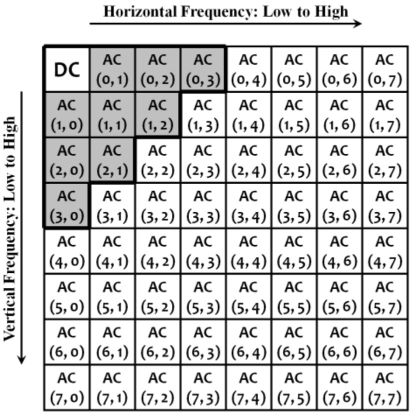
L. Y. Por *et al.* [5] present a method that stems from a mixture of inter-word and inter-paragraph spacing text-steganography techniques; they promise a higher capacity of integration and a lower detection-sensibility of the hidden data. The message is concealed in a dynamic generated cover in function of the length of the secret message, and which allows almost 60% increase in the capacity on integration compared with the traditional approaches. Nonetheless, this method still needs further examination of the robustness against attacks especially that there exists a wide variety of featured text-editors that could allow the abolition of the hidden data.

The authors in [6] set forth a digital watermarking application that aims at improving land-cultivation effectiveness throughout land consolidation; the improvement is reflected by cutting down the time-delay to half and drastically reducing the cost of the overall process. The proposed watermarking method is and enhancement of the well-known LSB-substitution algorithm with the objective of securing remote sensing images [20], which host the concealed data of the land reorganization planning-map. Because tampering is not affordable in such application, the presented method defies, from a statistical viewpoint, the dilemma of capacity of integration vs. invisibility of the watermark by compressively encoding the data, in a lossless manner, prior to the insertion stage using exclusive-OR encryption or scrambling preprocessing. The preprocessing benefits from the intrinsic properties of the image planning-map and achieves a 16-level indexed-color matching which allows a tremendous downsizing of by almost 85% of the original data. Additionally, distortion tolerance and Bit-Error-Ratio are pledged via an optimal adjustment process, thus ensuring a high-level of robustness against two common attacks, JPEG compression and additive noise arising from transmission errors.

4 Watermarking Algorithm

4.1 Watermark Insertion Using Nine AC Coefficients

We will estimate the AC coefficients of a center block by using dequantized DC values of a 3x3 neighborhood of 8x8 blocks. The estimation will encompass 9 coefficients instead of 5. The reason is that the third diagonal of the zigzag scan exhibits values almost of the same order compared with the second diagonal but significantly higher than the fourth one; this applies to the majority of images and it is to be underlined when images present sharp contrasts between adjacent pixels, such as textual or iconic graphics.



DC	AC (0, 1)	AC (0, 2)	AC (0, 3)	AC (0, 4)	AC (0, 5)	AC (0, 6)	AC (0, 7)
AC (1, 0)	AC (1, 1)	AC (1, 2)	AC (1, 3)	AC (1, 4)	AC (1, 5)	AC (1, 6)	AC (1, 7)
AC (2, 0)	AC (2, 1)	AC (2, 2)	AC (2, 3)	AC (2, 4)	AC (2, 5)	AC (2, 6)	AC (2, 7)
AC (3, 0)	AC (3, 1)	AC (3, 2)	AC (3, 3)	AC (3, 4)	AC (3, 5)	AC (3, 6)	AC (3, 7)
AC (4, 0)	AC (4, 1)	AC (4, 2)	AC (4, 3)	AC (4, 4)	AC (4, 5)	AC (4, 6)	AC (4, 7)
AC (5, 0)	AC (5, 1)	AC (5, 2)	AC (5, 3)	AC (5, 4)	AC (5, 5)	AC (5, 6)	AC (5, 7)
AC (6, 0)	AC (6, 1)	AC (6, 2)	AC (6, 3)	AC (6, 4)	AC (6, 5)	AC (6, 6)	AC (6, 7)
AC (7, 0)	AC (7, 1)	AC (7, 2)	AC (7, 3)	AC (7, 4)	AC (7, 5)	AC (7, 6)	AC (7, 7)

Fig. 2 – DCT coefficients in one block

Significant energy of the image is stored in the DC coefficients which are also referred to as the brightness coefficients (low frequency). The AC coefficients (high frequency) are referred to as the texture coefficients in the image and exhibit a high percentage of dark colors. A small variation of their value will result in a significant change in the image which makes them inappropriate to convey data. Thus, to carry data, the idea for watermarking is to estimate new AC coefficients that depend on the DC values.

Based on 3x3 neighborhoods of 8x8 blocks, we will use the following equations to estimate the AC coefficients. For instance, AC (0, 1) will be considered to be the central block of another virtual group of 3x3 blocks. This strategy will allow extending the coefficient prediction from five coefficients to nine.

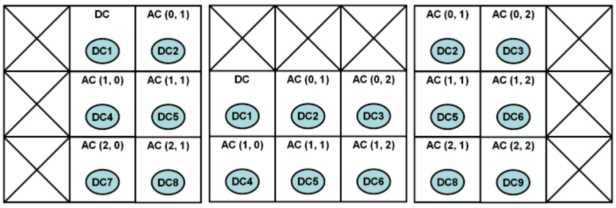


Fig. 3 – AC Coefficients Estimation

As we see in the middle block of Fig. 3 above, the upper corner does not exist, thus AC (0,

1) depends on the two other corners DC4 and DC6 [45] whereas AC (1, 1) is a center block with four corners thus, it is function of DC1, DC3, DC7, and DC9 and so forth for the remaining coefficients. This will yield the equations for AC estimation using the zigzag approach:

$$\begin{cases} AC(0,1) = 0.1423x\,(DC4 - DC6) \\ AC(1,0) = 0.1423x\,(DC2 - DC8) \\ AC(2,0) = 0.03485x\,(DC2 + DC8 \;\; 2\text{ x }DC5) \\ AC(1,1) = 0.0202x\,(DC1 - DC3 + DC9 - DC7) \\ AC(0,2) = 0.03485x\,(DC4 + DC6 - 2\text{ x }DC5) \\ AC(0,3) = 0.01779x\,(DC4 + DC6 - \; 2\text{ x }DC5) \\ AC(1,2) = 0.01779x\,(DC2 - DC8) \\ AC(2,1) = 0.01779x\,(DC4 - DC6) \\ AC(3,0) = 0.01779x\,(DC4 + DC6 - \; 2\text{ x }DC5) \end{cases} \quad (1)$$

4.2 Watermark Encryption: Scrambling

The algorithm is based on modulating the AC coefficients by a small amplitude delta (Δ) that will correspond to a message by setting an appropriate reference scale. Thus, each AC coefficient will carry one bit of information. Δ is chosen and adjusted for each diagonal in order to keep the watermark transparent and robust. Consequently, if for each 8x8 blocks we have one byte of data then the capacity of insertion can be computed by simply dividing the host image's size by 72. This distribution lends itself to the nature of the information to be hidden since for data, whether text-based or image-based, useful information is coded as multiples of a byte. Fig. 3 below shows a block diagram that describes the watermarking algorithm.

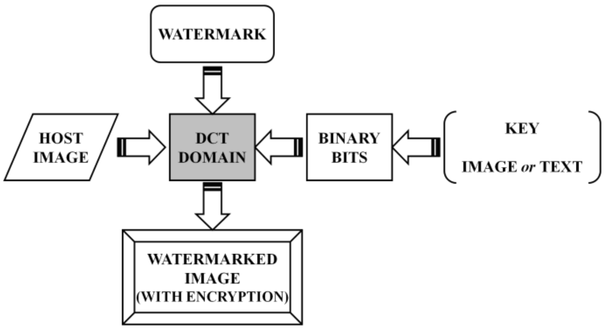


Fig. 3 – Block Diagram for Watermarking

In order to secure the confidentiality of the hidden data, the watermark is scrambled at the stage of its insertion [21]. In [34] and [35] the watermark is scrambled using the Arnold Transform in two interesting different ways. The novelty in our approach is to embed the key in the image itself hence offering two possibilities for extraction and copyright protection. The idea of the scrambling is simple and states that each bit of the watermark is inserted based on the binary values of each bit of the key. Consequently, the rule for watermarking is not kept the same while maintaining a high level of simplicity. Moreover, the key could be an image or a text from any language and the size of it (image or text) could be almost arbitrary. The only practical constraint is that the image or text that constitutes the key could be inserted in the host image. Practically, the key size could be calculated using the following formula: size (key) ≤ size (host image) /576.

Fig. 4 below shows a block diagram of the algorithm for scrambling the watermark at the insertion stage.

$$\begin{array}{ll} key\_bit = 0 & \begin{cases} AC > AC' + \Delta, & \text{to embed bit 1} \\ AC < AC' + \Delta, & \text{to embed bit 0} \end{cases} \\ key\_bit = 1 & \begin{cases} AC > AC' + \Delta, & \text{to embed bit 0} \\ AC < AC' + \Delta, & \text{to embed bit 1} \end{cases} \end{array}$$

Fig. 4 – Algorithm for watermark scrambling

4.3 Watermark Extraction

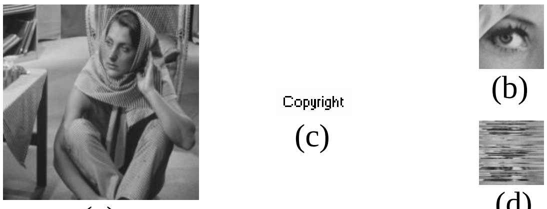
The watermark extraction process is spontaneous and can be determined by simply reversing the process of watermarking described in the section above. The original image is not required for watermark extraction. When AC is compared with its predicted value, AC' in the watermarked image, the extracted bit is 0 or 1 according to the algorithm shown in Fig. 4 above.

It is noteworthy to point out that the aforementioned algorithm for scrambling the watermark is the simplest one and one could imagine innumerable sophisticated versions of it. The novelty of our approach is a high flexibility in securing the hidden data in the sense that the options are unrestricted compared with the Arnold Transform where the method is frigid and an experienced hacker could crack it after some attempts. Hence, even an attacker depicts or intercepts the watermark, it is almost impossible to "guess" the "reverse transform" without possessing the key. This implies that the level of security in our approach is strengthened and reinforced at 3 different layers: the source of the key (any image or text), the arbitrary length of the key and a random scrambling algorithm.

5 Simulation Results

In order to test the proposed algorithm, we chose three still grayscale bitmap images. The first one (Barbara, 512x512) represents the host image, the second one (Lena's eye cropped, 3.5 KB) is the watermark to be embedded and the third one ('copyright', 0.4 KB) is used as the key as shown in Fig. 5 below.

At the beginning, the watermark was embedded with a neutral key, i.e. without scrambling. This was simply implemented by setting an array of binary zeros of appropriate size. This array was the source that gave the key bits to the algorithm. The watermark was successfully extracted with a PSNR of about 29.7689



(a) (b) (c) (d)

Fig. 5 – (a) Host, (b) watermark, (c) Key, (d) scrambled watermark

Next we used the center image above (c) as a key and we scrambled the watermark at the moment of implantation. An attempt was made to extract the watermark without the use of the key and showed that it is impossible to reveal the hidden data. This could be noticed on image (d) of Fig. 5 above which reveals a totally scrambled watermark. When the appropriate key was used, the watermark could be extracted successfully with a PSNR of approximately 28.9734

The aforementioned simulation tests were repeated with different host images (Lena, Cameraman, etc.) and all simulation results revealed that watermarking was transparent with an acceptable PSNR, decreasing by 3% for the worst case.

The watermarking algorithm was also tested using text messages for watermark and also text for key. Table 1 below shows a summary of the simulation results:

Table 1 – Simulation Results and PSNR for text-based watermarking

Image	Size	Bits inserted	PSNR
Cameraman	256x256	640	28.9167
IC	256x256	640	31.4378
Nodules	366x389	960	32.0462
Moon	537x358	1152	25.7725
Tire	232x205	576	22.3368

All watermarked images above were also subjected to some common signal processing and simulation results exhibit a high margin of robustness against these attacks. This result was expected since DC values are not changed and AC coefficients are estimated using these DC values. This makes the watermarking method intrinsically robust to signal processing.

6 Conclusion

In this paper we presented a new algorithm for watermarking still images in the DCT domain. The novelty of this approach is multifaceted. The main advantages of the proposed approach can be summarized as follows: (a) increased capacity of insertion by 60% while keeping the imperceptibility of the watermark; (b) the watermark is scrambled at the stage of insertion to ensure confidentiality against malign attacks; (c) enhanced security of the concealed data with a 3-level plan as mentioned in Section 4 of the paper; (d) simplicity and flexibility of the proposed algorithm are the same as for its predecessors.

The simulation results that were carried out demonstrated good performance of the algorithm in terms of blocking artifacts and PSNR which makes it a good choice for self-reference watermarking where security and confidentiality criteria are important.

References:

[1] Y. Govindharajan, S. Dakshinamurthi, Copyright Protection Protocols for Copyright Protection Issues, *WSEAS Transactions on Computer Research*, Vol. 3, No. 4, 2008, pp. 242-251.

[2] V. Saxena, J. P. Gupta, A Novel Watermarking Scheme for JPEG Images, *WSEAS Transactions on Signal Processing*, Vol. 5, No. 2, 2009, pp. 74-84.

[3] C. Atupelage, K. Harada, Perceptible Content Retrieval in DCT Domain and Semi-Fragile Watermarking Technique for Perceptible Content Authentication, *WSEAS Transactions on Signal Processing*, Vol. 4, No. 11, 2008, pp. 627-636.

[4] L. Y. Por, W. K. Lai, Z. Alireza, T. F. Ang, M. T. Su, and B. Delina, StegCure: A Comprehensive Steganographic Tool Using Enhanced LSB Scheme, *WSEAS Transactions on Computers*, Vol. 7, No. 8, 2008, pp. 1309-1318.

[5] L. Y. Por, T. F. Ang, and B. Delina, WhiteSteg: A New Scheme in Information Hiding Using Test Steganography, *WSEAS Transactions on Computers*, Vol. 7, No. 6, 2008, pp. 735-745.

[6] L. Li, C. Zhang, M. Liang, D. Li, Data Protection for Land Consolidation with Distortion Tolerable LSB Watermarking, *WSEAS Transactions on Information Science and Applications*, Vol. 6, No. 3, 2009, pp. 427-436.

[7] A. Khashman, and K. Dimililer, Image Compression using Neural Networks and Haar Wavelet, *WSEAS Transactions on Signal Processing*, Vol. 4, No. 5, 2008, pp. 330-339.

[8] Z. Brahimi, H. Bessalah, A. Tarabet, and M. K. Kholladi, Selective Encryption Techniques of JPEG2000 Codestream for Medical Images Transmission, *WSEAS Transactions on Circuits and Systems*, Vol. 7, No. 7, 2008, pp. 718-727.

[9] L. Chaari, M. Fourati, N. Masmoudi, and L. Kamoun, Image Transmission Quality Analysis Over Adaptive BCH Coding, *WSEAS Transactions on Communications*, Vol. 7, No. 6, 2008, pp. 584-593.

[10] Y. Zhang, Blind Watermark Algorithm Based on HVS and RBF Neural Network in DWT Domain, *WSEAS Transactions on Computers*, Vol. 8, No. 1, 2009, pp. 174-183.

[11] P. Kumsawat, K. Attakitmongcol, and A. Srikaew, An Optimal Robust Digital Image Watermarking Based on Genetic Algorithms in Multiwavelet Domain, *WSEAS Transactions on Signal Processing*, Vol. 5, No. 1, 2009, pp. 42-51.

[12] C. Chemak, J.-C. Lapayre, and M.-S. Bouhlel, A New Scheme of Image Watermarking Based on 5/3 Wavelet Decomposition and Turbo-Code, *WSEAS Transactions on Biology and Biomedicine*, Vol. 4, No. 4, 2007, pp. 45-52.

[13] G. Xie, and H. Shen, Rotation-Invariant Log-Polar Transform and its Application in Watermarking, *WSEAS Transactions on Information Science and Applications*, Vol. 1, No. 5, 2004, pp. 1127-1133.

[14] D. Osborne, D. Rogers, and D. Abbott, Embedded Watermarking for Wireless Image Content Authentication, *WSEAS Transactions on Communications*, Vol. 4, No. 7, 2005, pp. 505-513.

[15] K.-M. Hung, A Novel Robust Watermarking Technique Using IntDCT Based AC Prediction, *WSEAS Transactions on Computers*, Vol. 7, No. 1, January 2008, pp. 16-24.

[16] D. Dorel, Encrypting Messages with Visual Key, *WSEAS Transactions on Computers*, Vol. 8, No. 5, 2009, pp. 757-766.

[17] J.-T. Kim, D.-W. Kim, J.-S. Oh, H. Lim, and H.-K. Song, An Image Coding Technique by Variable Block Size and Region Compensation In DCT Domain, *WSEAS Transactions on Computers*, Vol. 5, No. 5, 2006, pp. 904-909.

[18] M. Prasad.R and S. Koliwad, A Comprehensive Survey of Contemporary Researches in Watermarking for Copyright Protection of Digital Images, *International Journal of Computer Science and Network Security*, Vol. 9, No. 4, 2009, pp. 91-107.

[19] S. Saryazdi and H. Nezamabadi-pour, A Blind Digital Watermark in Hadamard Domain, *World Academy of Science, Engineering and Technology*, Vol. 3, 2005, pp. 126-129.

[20] B.P. Kumari, V.P.S. Rallabandi, Modified Patchwork-Based Watermarking Scheme for Satellite Imagery, *Signal Processing*, Vol. 88, No. 4, 2008, pp. 891-904.

[21] D. Van De Ville, R. Van de Walle, W. Philips, and I. Lemahieu, Image scrambling using 2D DPSS, *Advances in Signal Processing, Robotics and Communications*, WSES Press, 2001, pp. 39-44.

[22] W.-P. Fang, Combining Copyright Protection and Data Hiding – A Sensitive Transformation Approach, *Proceedings of the 6th WSEAS International Conference on Signal Processing, Computational Geometry & Artificial Vision*, Greece, August 21-23, 2006, pp. 45-49.

[23] M.-S. Wang and W.-C. Chen, DCT-domain Copyright Protection Scheme Based on Secret Sharing Technique, *Proceedings of the 7th WSEAS International Conference on Signal Processing, Computational Geometry & Artificial Vision*, Greece, August 24-26, 2007, pp. 107-111.

[24] H. Seddik, M. Sayadi, and F. Fnaiech, A New Watermarking Scheme, Robust Against JPEG Compression and Some Asynchronous Attacks Based on Hough Transform, *Proceedings of the 5th WSEAS International Conference on Multimedia, Internet and Video Technologies*, Greece, August 17-19, 2005, pp. 165-170.

[25] K. Sumitomo, M. Nakano, and H. Perez, Image Authentication and Recovery Scheme Based on Watermarking Technique, *2nd WSEAS International Conference on Computer Engineering and Applications (CEA'08)*, Mexico, January 25-27, 2008, pp. 94-99.

[26] P. Singh, S. Batra, and H. Sharma, Steganographic Methods Based on Digital

Logic, *Proceedings of the 6th WSEAS International Conference on Signal Processing*, Texas, USA, March 22-24, 2007, pp. 157-162.

[27] Y.I. Khamlichi, M. Machkour, K. Afdel, and A. Moudden, Medical Image Watermarked by Simultaneous Moment Invariants and Content-Based for Privacy and Tamper Detection, *6th WSEAS International Conference on Multimedia Systems & Signal Processing*, China, April 16-18, 2006, pp. 109-113.

[28] A. Samcovic, and J. Turan, Digital Image Watermarking by Spread Spectrum, *Proceedings of the 11th WSEAS International Conference on Communications*, Greece, July 26-28, 2007, pp.29-32.

[29] K.-M. Hung, Y.-T. Wang and C.-H Yeh, A Robust Watermarking Technique for Copyright Protection of Digital Images, *Proceedings of the 2007 WSEAS International Conference on Computer Engineering and Applications*, Australia, January 17-19, 2007, pp. 248-253.

[30] X. Wang, Y Ou-Yang, and H.-M. Gu, A Remote Sensing Image Self-Adaptive Blind Watermarking Algorithm Based on Wavelet Transformation, *Proceedings of the 7th WSEAS International Conference on Signal, Speech and Image Processing*, China, September 15-17, 2007, pp. 76-82.

[31] A. Hassan and M. S. Baig, Parallel Implementation of Spread Spectrum Based Oblivious Visual Watermarking Using Efficient DWT, *Proceedings of the 6th WSEAS International Conference on Applied Computer Science*, Spain, December 16-18, 2006, pp. 473-477.

[32] C.A. Gonzales, L. Allman, T. McCarthy and P. Wendt, DCT Coding for Motion Video Storage Using Adaptive Arithmetic Coding, *Signal Processing: Image Communication, No. 2*, Elsevier, 1990, pp. 145-154.

[33] Y. Wang and A. Pearmain, AC Estimation-Based Image Watermarking Method, *Proceedings of WIAMIS*, 21-23 April 2004.

[34] R.M. Zhao, H. Lian, H.W. Pang and B.N. HU, A Blind Watermarking Algorithm Based on DCT, *Second International Symposium on Intelligent Information and Technology Application IITA'08*, 20-22 December 2008, pp. 821-824.

[35] A. Hu and N. Chen, A Blind Watermarking Algorithm for Color Image Based on Wavelet Transform and Fourier Transform, *The 9th International Conference for Young Computer Scientists ICYCS'08*, 18-21 November 2008, pp. 1453-1458.

[36] K. Veeraswamy, B. Chandra Mohan and T. Jyothirmayi, An Image Compression Scheme Using AC Predictions, *International Conference on Computational Intelligence and Multimedia Applications ICCIMA'07*, Proc. Vol. 3, 13-15 December 2007, pp. 2530-2535.

[37] S. Saryazdi and M. Demehri, A Blind DCT Domain Digital Watermarking, *SETIT*, 27-31 March 2005, pp. 55-57.

[38] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, Pearson Education, Third Edition, 2008.

[39] I. J. Cox, J. Kilian, T. Leighton and T. Shamoon, Secure Spread Spectrum Watermarking for Multimedia, *IEEE Transactions on Image Processing*, Vol. 6, No. 12, December 1997, pp. 1673-1678.

[40] B. Chen and G. Wornell, Quantization Index Modulation: A Class of Probably Good Methods for Digital Watermarking and Information Embedding, *IEEE Transactions on Information Theory*, Vol. 47, No. 4, May 2001, pp. 1423-1443.

[41] W. Diffie and M. Hellman, Multi-User Cryptographic Techniques, *AFIPS Proceedings 45*, June 1976, pp. 109-112.

[42] http://en.wikipedia.org/wiki/Cryptography

[43] C. Shannon and W. Weaver, *The Mathematical Theory of Communication*, University of Illinois Press, 1963.

[44] J. C. Judge, *Steganography: Past, Present, Future*, SANS Institute, Information Security Reading Room, October 2003.

[45] K. Veeraswamy and S. Srinivas Kumar, Adaptive AC-Coefficient Prediction for Image Compression and Blind Watermarking, *Journal of Multimedia*, Vol. 3, No. 1, May 2008, pp. 16-22.

[46] H. Aboalsamh, H. Mathkour, S. Dokheekh, M. Mursi, and G. Assassa, An Improved Steganalysis Approach for Breaking the F5 Algorithm, *WSEAS Transactions on Computers*, Vol. 7, No. 9, 2008, pp. 1447-1456.

[47] Gary C. Kessler, An Overview of Steganography for the Computer Forensics Examiner, *Forensics Science Communications*, Vol. 6, No. 3, July 2004.

[48] C. Hosmer, and C. Hyde, Discovering Covert Digital Evidence, *Digital Forensic Research Workshop (DFRWS)*, August 2003.

[49] G. Langelaar, I. Setyawan, R.L. Lagendijk, Watermarking Digital Image and Video Data, *IEEE Transactions on Signal Processing*, Vol. 17, September 2000, pp 20-43.