Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: July 2021 **2022, 19(1): 197-207** **E-ISSN: 2411-7986**

DOI: http://dx.doi.org/10.21123/bsj.2022.19.1.0197

An Enhanced Approach of Image Steganographic Using Discrete Shearlet Transform and Secret Sharing

Yasir Ahmed Hamza [1]* ***Nada Elya Tewfiq*** [1] ***Mohammed Qasim Ahmed*** [2]

[1] Department of Computer Science, College of Computer and IT, Nawroz University, Duhok, Iraq
[2]Department of Computer Science, College of Education, University of Alhamdaniya, Mosul, Iraq
Corresponding author: yasir.ahmed@nawroz.edu.krd,nada.tawfiq@nawroz.edu.krd ,m.kassim@uohamdaniya.edu.iq
*ORCID ID: https://orcid.org/0000-0002-2191-2370 *,https://orcid.org/0000-0003-0992-8481 ,https://orcid.org/0000-0002-1481-8298

Received 4/12/2019, Accepted 4/11/2020, Published Online First 20/7/2021, Published 1/2/2022

Abstract

Recently, the internet has made the users able to transmit the digital media in the easiest manner. In spite of this facility of the internet, this may lead to several threats that are concerned with confidentiality of transferred media contents such as media authentication and integrity verification. For these reasons, data hiding methods and cryptography are used to protect the contents of digital media. In this paper, an enhanced method of image steganography combined with visual cryptography has been proposed. A secret logo (binary image) of size (128x128) is encrypted by applying (2 out 2 share) visual cryptography on it to generate two secret share. During the embedding process, a cover red, green, and blue (RGB) image of size (512x512) is divided into three layers (red, green and blue). The blue layer is transformed using Discrete Shearlet Transform (DST) to obtain its coefficients. The first secret share is embedded at the coefficients of transformed blue layer to obtain a stego image. At extraction process, the first secret share is extracted from the coefficients of blue layer of the stego image and XORed with the second secret share to generate the original secret logo. According to the experimental results, the proposed method is achieved better imperceptibility for the stego image with the payload capacity equal to (1 bpp). In addition, the secret logo becomes more secured using (2 out 2 share) visual cryptography and the second secret share as a private key.

Key words: Blue Layer, Discrete Shearlet Transform, Image Steganography, Stego Image, Secret Sharing.

Introduction:

Nowadays, millions of users are able to transmit the digital media through the internet easily. This feature of the internet leads to a number of challenges and threats regarding the security of transmitted media contents such as (copyright protection, media authentication and integrity verification) [1-4]. Therefore, data hiding and cryptography methods are to be the essential requirements for protecting the contents of digital media [3]. Data hiding methods perform the security for the digital media by embedding a secret data in another digital media called a cover media [5]. In other word, they make an existence of the secret data invisible at the cover media [6]. While, cryptography methods change the secret data into illegible form [7-8], some applications of data hiding are designed by combining them with cryptography [9,10].

Data hiding approaches can be divided into two main methods, namely steganography and watermarking [3]. Steganography is similar to watermarking in general concept of data hiding. That means, they are hidden in an existence of the secret data by camouflaging it within another digital media such as (image, video, text or sound) [6]. However, steganography is different from watermarking according to three main requirements: imperceptibility, payload capacity and robustness [4, 11]. Imperceptibility means the cover media should keep the perceptually of stego media (cover media after applying embedding process) after the secret data embeds in it [7, 12]. Generally, stego media such as image must preserve its visual quality from a distortion that are generated during the secret data embedding process. Payload capacity stands for a number of the secret data bits that can be embedded in the cover media [13].

Robustness refers to an ability of the secret data to resist against the attack such as (common image processing, compression,… etc) [4].

The requirements mentioned above are used as evaluation measurements for data hiding approaches. Steganography techniques especially image steganography are concentrated on the high stego image imperceptibility and the maximum payload capacity [7]. Whenever, watermarking methods focus on the robustness as an essential requirement [7, 14]. The most image steganographic methods aim to enhancing the stego image imperceptibility and maximizing the payload capacity. However, there is a trade-off between these requirements when designing the image steganography application. Increasing the embedding bits of secret data may lead to degradation in the stego image quality and it decreases the stego image imperceptibility [1, 15]. In addition, there is another problem related to the secret data may be subject to various kinds of the stego image attacks and it allows an adversary to extract/detect the embedded secret data bits [6]. Therefore, a hybrid method of steganography and cryptography can achieve confidentiality for the hidden secret data [10].

In this paper, a new approach of combined image steganography and cryptography has been proposed. The suggested scheme is concentrated on the two main requirements of image steganography (imperceptibility, and payload capacity). Also, the security of the embedded secret logo can be achieved using the visual cryptography. Consequently, the proposed method is divided into three main processes. Firstly, the secret logo is encrypted using (2 out 2 share) visual cryptography to generate two secret shares (one for embedding process and another used as a private key for an extraction processing). Secondly the embedding process, a cover image is divided into (red, green and blue (RGB)) layers and the blue layer is transformed into frequency domain using discrete shearlet transform (DST). Then, one of the secret shares is embedded in the coefficients of the blue layer to generate the stego image. Finally, the embedded secret share is extracted from the coefficients of blue layer of the stego image and XORed with the second secret share to obtain the original secret logo. According to the experimental results, the suggested approach achieves a better image quality and high value of Peak Signal to Noise Ratio (PSNR). In addition, the proposed method attains best embedding capacity equal to one bit per pixel (bpp) and the confidentiality of secret logo is improved by applying visual cryptography.

This paper is organized as follows. The pervious proposed methods of data hiding are demonstrated in the related works. The theoretical background of shearlet system and its transformations is explained in the shearlet transform. The (2 out 2 share) scheme for the secret logo is described in visual cryptography. The proposed method illustrates the secret logo embedding and extraction processes of a new image steganographic approach. An evaluation of the suggested method performance is discussed in the experimental results. Finally, conclusion summarizes the contributions and limitations of the proposed method followed by references.

Related Works

Based on the survey, some of the proposed methods that are based on DST have been applied for image watermarking. As mentioned before, image watermarking methods are generally concentrated on the robustness for the embedded watermark due to using it for copyright protection or integrity verification of digital images. In this study, a new method of image steganography that depends on DST has been suggested. Therefore, this approach can be the first study based on DST for image steganography. Unfortunately, there are no studies that used DST to design image steganographic approaches.

There are a several methods of data hiding have been proposed by researchers. Some of these methods are applied at spatial domain of images [5, 11, 15] and others are used in transform domain of images [1, 3, 4, 9, 12, 13, 16]. In [1], the researchers suggested a method of image watermarking that based on DST. A cover image is decomposed by applying DST. Then, Chou's visual model is used to estimate the Just Noticeable Distortion (JND) values for each coefficient of the decomposed cover image. At embedding process, the most significant and largest coefficient values of JND are used for embedding a watermark bits. Finally, the watermarked image is obtained by applying Inverse DST. Based on the experimental results, the proposed method achieves high imperceptibility for the watermarked image and good robustness for the watermark.

Priya et al [3] proposed a medical image watermarking using Integer Wavelet Transform (IWT). A cover image is transformed using IWT into four sub-bands and the low frequency sub-band is interpolated using neighbor nearest interpolation. An electronic patient information is used as a watermark and it is embedded at the interpolated low frequency sub-band to generate a watermarked image. This method presents a good imperceptibility as its experimental results. Zhao et al [4] suggested another method of image watermarking. The cover image is transformed into

directional sub-bands by applying nonsubsample shearlet transform. The strongest directional sub-band is selected for embedding process and it transformed into a singular value matrix using Singular Value Decomposition (SVD). A watermark is embedded at the singular value matrix to obtain a watermarked image. The result of proposed method shows high imperceptibility and more robustness.

Ananth and Sudhakar [5] proposed a combined technique of image steganography and cryptography. A watermark is encoded by applying barcode encoder and it embedded at the cover image using Least Significant Bit (LSB) substitution method. The proposed method presents good imperceptibility for a stego image and increases the secrecy of the secret data. In [9], Sun and Guo proposed hybrid method of cryptography and steganography. The cover image is decomposed into low pass sub-bands and high pass sub-bands using Contourlet Transform (CT). The suitable high pass sub-bands are selected for embedding process and they are divided into 4x4 blocks. The secret image is encrypted using Hill Cipher and it embedded at each block using the coefficient 2-LSB. All blocks are corrected by using 2^k correction method and they merged to obtain a stego image. According to its results, the proposed method achieves confidentiality for the secret image and better imperceptibility for stego image. Sun [11] suggested a new method of image steganography based on Bit-plane complexity segmentation (BPCS). A cover image and a secret image are transformed from Pure Binary Code (PBC) into Canonical Gray Code (CGC). According to its results, this method presented better PSNR value and high embedding capacity. Ahmaderaghi et al [12] proposed a blind image watermarking approach-using DST. The method is implemented the decision theory for blind extraction of watermark. For this reason, a Probability Density Function (PDF) is applied on the distribution of DST coefficients for different sub bands using Laplacian channel. Finally, maximum likelihood detection that depends on Laplacian model for DST coefficients is applied under the detection rules of Neyman-Pearson criterion for improving the robustness. The experimental results show that the proposed method achieves good imperceptibility, improved payload capacity and superior robustness. In [13], Hemalatha et al presented a method of image steganography based on IWT. A cover RGB image is converted into YCbCr color system. Then, IWT is applied on Cb, Cr channels and the secret audio signal. Two bits of the secret audio signal are embedded at 2nd and 3rd bit planes of high frequency of the Cb and Cr coefficients. Based on its results, the proposed approach achieves good imperceptibility and robustness. Hamza [15] presented a method of image steganography using LSB. The secret logo is scrambled using Arnold's Cat Map and Blum Blum Shub. The cover image is divided into blocks and entropy of each block is calculated. The block of maximum entropy is selected to embed to one bit of the secret logo at 1st LSB of the selected block. According to its experimental results, the proposed method achieves better imperceptibility and high security. Mostaghim and Boostani [16] proposed a method of image steganography using Discrete Wavelet Transform (DWT) and visual cryptography. A chaotic system is used to generate on secret share based on visual cryptography. Then, this secret share is XORed with a secret logo to generate a scrambled secret logo. A DWT is applied on a cover image and the scrambled secret logo is embedded at the low frequency coefficients of the cover image. Experimental results show that the suggested approach presents good imperceptibility and increases the security of the secret logo.

Shearlet Transform

Recently, shearlet is the most successful scheme for representing the multi-dimensional data such as (digital image) efficiently [17, 18]. It is able to represent the anisotropic features sparsely through the optimal encoding for some classes of multivariate data [18]. Shearlet provides new tools for analysis and processing massive dimensional data, which are limited in Fourier and wavelet system. It achieved an efficient computation and a number of shearing directions are not restricted when compared with a contourlet. In addition, it differs from directional filter bank that supports shearing size without any constraint [19]. Therefore, using a window with small sized cannot lead to lose its performance.

The Shearlet Transform (ST) is used to handle the image anisotropic and directional features. In addition, it is able to capture the geometric information of edges effectively [1, 18, 19]. ST can be described as affine function that contains a single mother of shearlet function [12]. The shear parameter that captured the direction of the singularities such as (lines and curves) is calculated according to scaling, shear and translation parameters. A Laplacian pyramid and directional filtering are used to apply the shearlet transform [1, 12]. For the cover image CI and mother function $\psi \in L^2(\mathbb{R}^2)$, ST of $CI \in L^2(\mathbb{R}^2)$ is the mapping [18, 19] defined by:

$$CI \to \mathcal{SH}\psi\, CI(a,s,t) = \langle CI, \psi\, a,s,t\rangle : a,s \in \mathbb{Z}, t \in \mathbb{Z}^2$$

This means, $\mathcal{SH}\psi$ maps the function CI to the coefficients $\mathcal{SH}\psi\, CI(a,s,t)$ associated with a as

scale ($a > 0$), s the orientation and t is the translation indices.

Shearlets can be obtained using dilating, shearing and translating [12, 19] on the mother function $\psi \in L^2(\mathbb{R}^2)$. The dilation is defined as matrix:

$A_a = \begin{pmatrix} a & 0 \\ 0 & \sqrt{a} \end{pmatrix}$ where $a \in \mathbb{R}^+$ and shear is defined by a matrix $S_s = \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix}$ where $s \in \mathbb{R}$. DST can be constructed by an appropriate sampling a continuous shearlet transform on a set S. Therefore, different approaches of the discrete shearlet systems have been proposed aiming to form an orthonoml basis or $\psi \in L^2(\mathbb{R}^2)$ of a tight frame [18, 19]. The mother function ψ of DST is defined as:

$$\mathcal{SH}(\psi) = \{\psi j, k, m = 2^{3/4j}\, \psi(S_k A_{2j} - m)\} : j, k \in \mathbb{Z}, m \in \mathbb{Z}^2 \quad (1)$$

A DST has been applied on a (blue layer) of the cover image (Lena) as shown in Fig.1. The blue layer only is transformed using DST because of this layer of the cover image will be used for secret share embedding process.

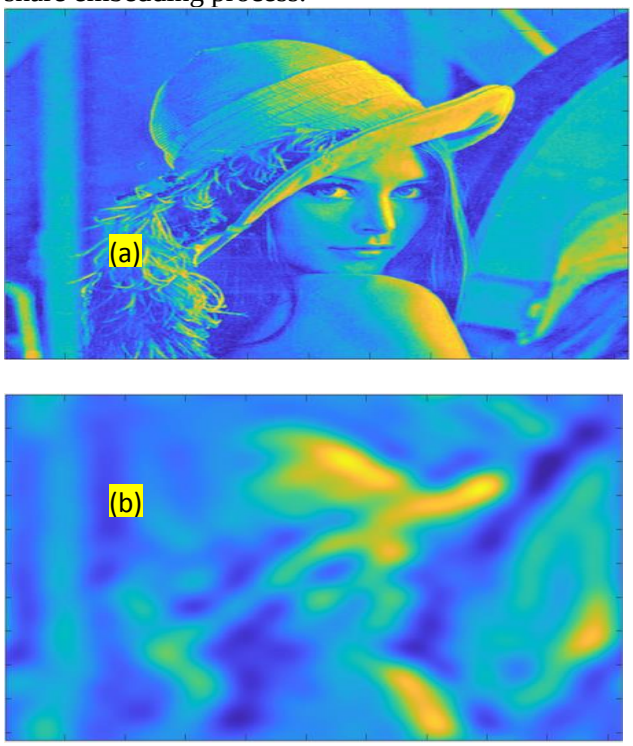


Figure 1. The cover image (Lena) after applying DST, (a) DST with scale *j=1*, (b) DST with scale *j=5*.

Visual Cryptography:

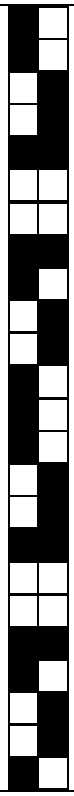
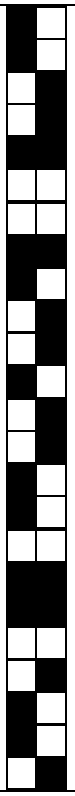
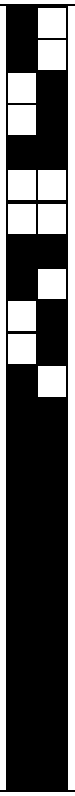
Visual cryptography is a method for encrypting the writing materials such as (handwritten notes or pictures) visually [20]. It maintains the secrecy of such data optimally. Naor and Shamir [20] are proposed (k, n) visual cryptography approach in 1994. An original image is split into (n) shares and any (k) shares that can be stacked together to reconstruct the original image [16]. A (2 out, 2 share) is the simplest method of visual cryptography that split the original binary image (black and white) into two secret shares. Each secret share is appeared completely as random pattern of the original binary image. The shares are given to each participant. Then to obtain the original image, the participants must stack the secret shares one above another one.

Visual cryptography achieves the confidentiality for the entire secret image by each secret share does not give any information about it and the original secret image is obtained only if the secret shares stack together. This method is divided into two processes: ciphering process and deciphering process. At ciphering process, a plain data such as binary-image is converted into a set of transparent images called shares. In deciphering process, these shares are stacked one above the other to generate the original binary-image. For this reason, the deciphering process is done using the human visual system and it does not need complex calculations [16, 20, 21]. To generate (2 out 2 share) for the secret-logo that used in embedding process. The following steps are applied on the secret-logo.

- Pick each pixel of the secret-logo and compare a color of pixel according to the following condition:
  - If the color of pixel is white, then select randomly a pair of the white color probabilities form Table 1 and put a first probability at a secret share one and a second probability or (offset) in a secret share two.
  - If the color of pixel is black, then choose randomly a pair of the black color probabilities form Table 1 and place a first probability in a secret share one and a second probability in a secret share two.
- The condition that mentioned above is repeated on the entire pixels of the secret-logo.
- The result is two secret shares.

Baghdad Science Journal
2022, 19(1): 197-207
P-ISSN: 2078-8665
E-ISSN: 2411-7986

Table 1. (2 out 2 share) visual cryptography scheme

Color	Share1 50%	Share2 50%	Stacked Share1 and Share2
White			
Black			

The proposed method is implemented the (2 out 2 share) scheme on the secret logo to generate two secret shares. A binary image of the secret logo with size (128x128) is spilt up into two secret shares; each one is randomly scrambled image of size (128x256). The width of each secret share will be resized to double during the process of generating it, because of the (2 out 2 share) scheme must put the probabilities for each color (white or black) according to the Table.1. The result of generating two secret shares for the secret logo shows in Fig.2.

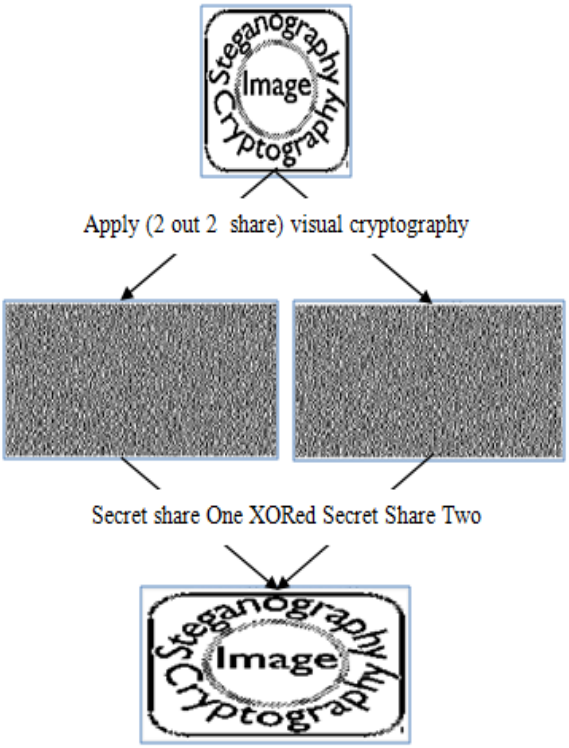


Figure 2: the secret shares generating method

Proposed Method

In this section of paper, the proposed approach of image steganographic is illustrated in details. The suggested method is divided into two main processes (embedding process and extraction process). During the embedding process, the cover image is partitioned into three layers (red, green, and blue). The blue layer is selected to embed the secret share one in it. The reason for choosing the blue layer because of Human Visual System (HVS) is less sensitive to modification at blue color. Also, the blue color achieves high value of PSNR for the proposed approach. Then, DST is applied on the blue layer to obtain its coefficients. The entire coefficients are used to embed the secret share one. The following formula is used to embed one bit of secret share at each coefficient:

$$BC'(i,j) = \begin{cases} BC(i,j) + S1(i,j), & S1(i,j) = 1 \\ BC(i,j) \quad , & S1(i,j) = 0 \end{cases} \quad (2)$$

Where *BC* is the coefficient of blue layer, *S1* is the bit of secret share one, $1 \leq i \leq 128$, and $1 \leq j \leq 256$. For the cover image of size (512x512), the secret share one is embedded (8) times in its blue layer coefficients. The modified blue layer *BC'* is combined with red and green layers to obtain the stego image. The block diagram of embedding process is shown in the Fig.3.

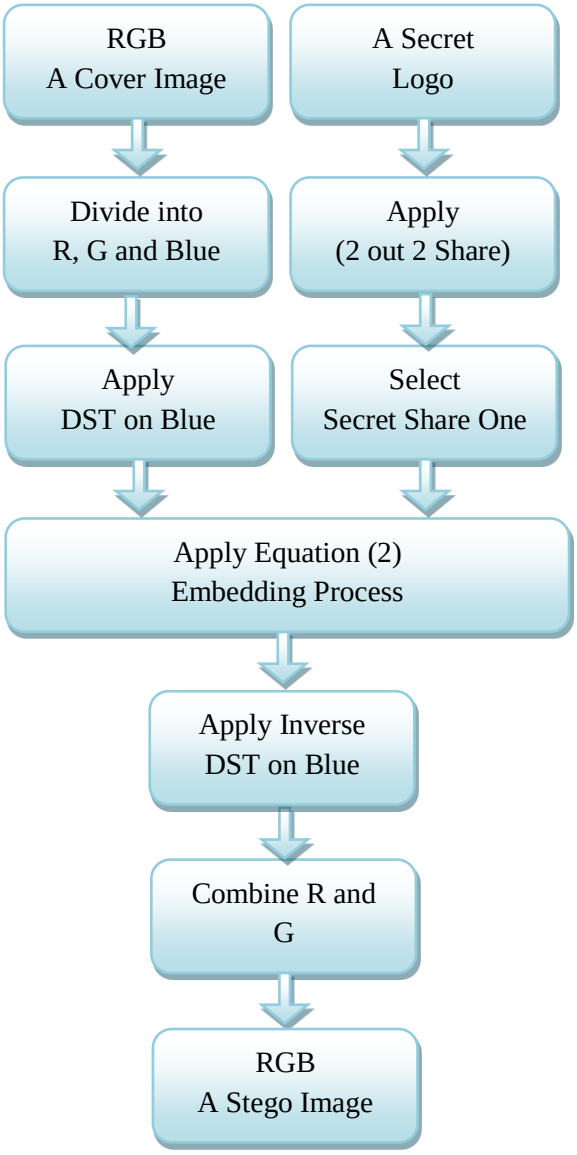


Figure 3. The block diagram for embedding process

At the extraction process, the stego image and the riginal cover image are partitioned into three layers (red, green, and blue). The blue layer of each one are transformed using DST. Then, the formula that defined below is used to extract one bit of secret share one from each coefficient:

$$S1(i,j) = \begin{cases} 1, & BC'_{stego} > BC_{cover} \\ 0, & BC'_{stego} = BC_{cover} \end{cases} \quad (3)$$

Where *BC* is the coefficient of blue layer (original cover), *BC'* is the coefficient of blue layer (stego) and *S1* is the bit of secret share one, $1 \le i \le 128$, and $1 \le j \le 256$. The secret share one can be extracted (8) times from the stego image of size (512x512). The extracted secret share one is XORed with a secret share two to obtain the original secret logo. Figure 4 shows the block diagram of extraction process.

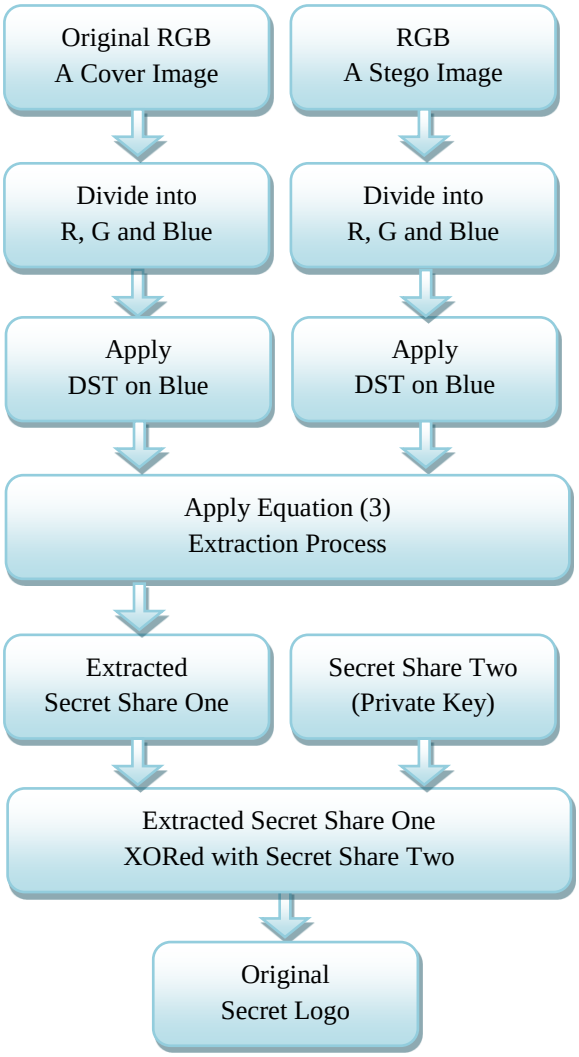


Figure 4. The block diagram for extraction process

Experimental Results

In this section, the proposed approach has been implemented by using MatlabR2019b that runs on Sony Vaio laptop, Intel Corei3-3227U CPU 1.9 GHz, 4 GB RAM, and Windows 10 Home 64-bit operating system, to evaluate its performance. Therefore, three programs have been written; the first program is used for secret share generating, the second program is applied for embedding process and the third program is employed for extraction process. The colored-images of size (512x512) are used as the cover images for testing and evaluating the suggested approach as shown in Fig.5. The secret logo is a binary image of size (128x128).

(a) Lena (b) Baboon (c) Airplane

(d) Boats (e) Tiffany (f) Peppers

Figure 5. the set of the cover images

During the embedding process, the secret share of size one is embedded (8) times in the coefficients of DST for the blue layer of the cover image and the stego image is obtained. As mentioned before, the embedding process causes distortion in the stego image. Therefore, mean square error (MSE) is used as measurement for calculating a statistical difference between the cover image and the stego image. The lower value of MSE refers to less distortion and high quality in the stego-image and vice versa. MSE can be computed by equation:

$$\text{MSE} = \frac{1}{M*N} * \sum_{i=1}^{m} \sum_{j=1}^{n} (CI(i,j) - SI(i,j))^2 \quad (4)$$

Where *CI* is the cover image and *SI* is the stego image. *M* and *N* is the size of each image and $1 \leq i \leq M$, and $1 \leq j \leq N$. PSNR is used to compute the impact on the image quality between cover image and stego image. If PSNR value is high, that means the better image quality of stego image and vice versa. A decibel (dB.) is PSNR metric. The following formula is used to calculate the PSNR:

$$\text{PSNR} = 10 * \log_{10}\left(\frac{255^2}{MSE}\right) \quad (5)$$

Structural similarity (SSIM) is used as a metric to measure the similarity between the cover image and the stego image. This measurement is developed to enhance the traditional measurements such as MSE and PSNR that have proven inconsistent for human eye perception [1]. Therefore, SSIM is more adaptable with nature of HVS [8]. The maximum value of SSIM is equal to 1 and it represents the identical between the cover image and the stego image.

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)} \quad (6)$$

where *x* is the cover image and *y* is the stego image. $\mu_x and\ \mu_y$ are the mean of *x* and *y*, $\sigma_x^2 and\ \sigma_y^2$ are the variance of *x* and *y*. (σ_{xy}) is the co-variance of *x* and *y*. $C_1 and\ C_2$ are two constants used for avoiding null denominator. The bpp can be calculated according to the following equation:

$$bpp = \frac{Number\ of\ embedded\ bits}{M*N} \quad (7)$$

where the number of the embedded bits are represented the total size of the secret share one that is embedded in the cover image. The size of the cover image is *(M=512 and N=512)*, that means the total size of it is equal to *512*512=262144* pixels. As mentioned before, the size of the secret share is (128x256) and the total bits is equal to *128*256= 32768* bits. During the embedding process, the secret share one will be embedded eight times in the blue layer coefficients and the total number of the embedded bits will become (*32768*8=262144 bits*). Consequently, each pixel of the blue layer will be hiding one bit of the secret share one. The payload capacity *=262144* bits and bpp=*262144/262144=1*. The values of MSE,

PSNR, SSIM and bpp after testing a performance of the proposed method are shown in Table 2.

Table 2. the values of MSE, PSNR, SSIM and bpp for each stego image.

Stego image	MSE	PSNR (dB.)	SSIM	Payload capacity (bits)
Lena	0.2500	54.15	0.9999	262144
Baboon	0.2500	54.15	0.9999	262144
Airplane	0.2517	54.13	0.9998	262144
Boats	0.2517	54.12	0.9596	262144
Tiffany	02501	54.14	0.9999	262144
Peppers	0.2516	54.12	0.9878	262144

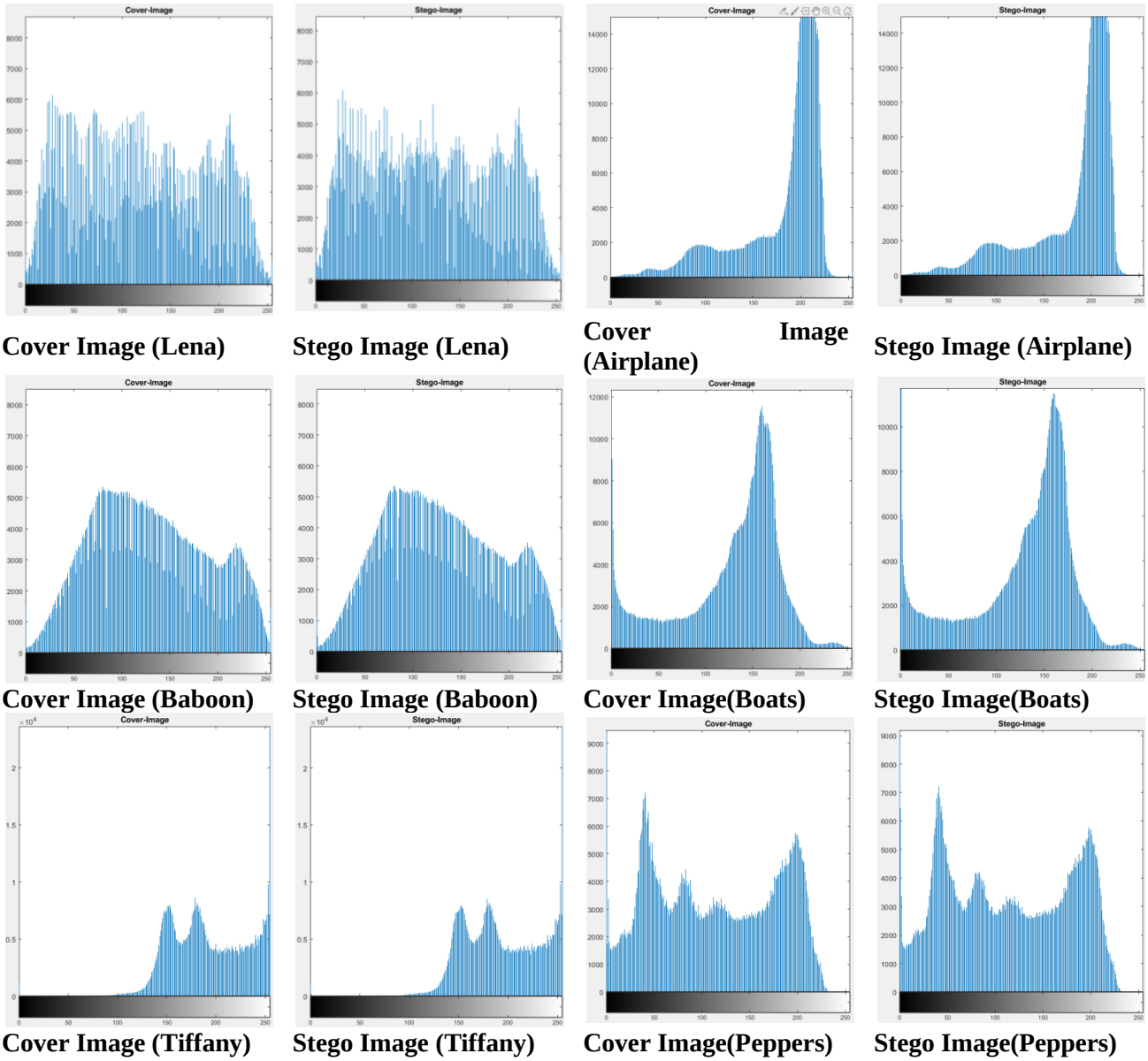
Another method for evaluating the proposed method can be done by comparing it with other methods that proposed in the related works. Table 3 shows the performance comparison between the suggested approach and another method that proposed by Sun and Guo [9]. Meanwhile, other methods that proposed in [1, 3, 4, 12] are the image watermarking. As mentioned early, image watermarking is different form image steganography in its essential requirement of robustness. The image steganography methods that proposed in [13] and [16] are tested by only one cover image "Lena" of size (512x512) with value of *PSNR=41.6* and payload capacity*=262,144 bits*. While, the second method values are *PSNR=63.34* and payload capacity *=58,339 bits*.

Table 3. Performance comparison of proposed method with another approach

Stego image	Proposed Method		Sun and Guo [9]	
	PSNR (dB.)	Payload capacity (bits)	PSNR (dB.)	Payload capacity (bits)
Lena	54.15	262144	53.28	131,072
Baboon	54.15	262144	52.66	131,072
Airplane	54.13	262144	51.35	131,072
Boats	54.12	262144	52.49	131,072
Tiffany	54.14	262144	N/A	N/A
Peppers	54.12	262144	52.96	131,072

According to the results of Table.2 and Table.3, the proposed method is achieved high value of PSNR for all stego images and it has been preserved the imperceptibility. The SSIM values for all stego images are approximately equal to one. That means, there are higher similarity between the cover image and the stego image. The payload capacity is (262144) bits for the stego image of size (512x512) which the rate of embedding equal to (*1 bpp*). However, the payload capacity for Sun and Guo [9] method is (131,072) bits and the embedding rate equal to (*0.5 bpp*). Therefore, the proposed method has achieved best value of payload capacity. The secret logo is attained more secrecy using (2 out 2 share) visual cryptography. In addition, the secret logo is split up into two secret shares: one secret share is embedded in the stego image and the second secret share is used as private key during the extraction process. Without this private key, the original secret logo cannot be obtained correctly.

Statistical steganalysis is used to detect abnormal modification in the structural characteristics of the stego image. Histogram analysis is one of the most important criteria for the statistical steganalysis [16]. A histogram of the stego image is compared with a histogram of the cover image to identify the distribution of pixels or the unusual shapes that occurred due to embedding process. In order to evaluate the proposed approach against the histogram analysis, the histograms for each cover image and stego image are calculated as shown in Fig.6. According to the Fig.6, the histogram of each image cover and its stego image is uniformity and there are usual shapes among them.



Cover Image (Lena) | Stego Image (Lena) | Cover Image (Airplane) | Stego Image (Airplane)

Cover Image (Baboon) | Stego Image (Baboon) | Cover Image(Boats) | Stego Image(Boats)

Cover Image (Tiffany) | Stego Image (Tiffany) | Cover Image(Peppers) | Stego Image(Peppers)

Figure 6. The histograms for each cover image and stego image

Conclusion:

In this study, a new method of image steganography has been proposed. the method is based on DST and secret sharing. According to the experimental results, the two main requirements of image steganography have been achieved: better imperceptibility and high embedding capacity. Based on histogram analysis, the histogram of each cover image and its stego image are in uniformity. Therefore, using DST instead of other transformations such as (wavelet, contourlet and discrete cosine) is the best for image steganography methods. Using (2 out 2 share) visual cryptography with one share as the private key is enhanced the security of secret logo. Because, if the attacker was able to extract the secret share one from the stego image, it could not obtain the original secret logo without the secret share two. Finally, the suggested approach is non-blind and it required the original cover image at the extraction process. Therefore, this limitation can be addressed for future works.

Authors' declaration:

- Conflicts of Interest: None.
- We hereby confirm that all the Figures and Tables in the manuscript are mine ours. Besides, the Figures and images, which are not mine ours, have been given the permission for re-publication attached with the manuscript.
- Ethical Clearance: The project was approved by the local ethical committee in Nawroz University.

Author's contributions statement:

- The contribution of each author in the submitted manuscript (MS) to the "Baghdad Science Journal" should be specified in the MS itself.

- The author(s) use(s) their initials to explain his/her contribution (FM Hassan collected the sample and analyzed all parameters,. etc.). Each authorship is expected to make substantial contribution to part of the MS from the conception of research to submitting the MS. All authors read the manuscript carefully and approve the final version of their MS.

References:

1. Ahmaderaghi B, Rincon J, Kurugollu F, Bouridane A. Perceptual Watermarking for Discrete Shearlet Transform. In proceedings of 2014 5th European Workshop on Visual Information Processing (EUVIP). Paris, France, IEEE, 2014: 1- 6.
2. Ansari AS, Mohammadi MS, Parvez MT. A Comparative Study of Recent Steganography Techniques for Multiple Image Formats. IJCNIS, 2019; 11(1):11-25.
3. PRIYA S, SANTHI B, RAJA MOHAN J. Medical Image Watermarking Technique Using Image Interpolation in Transform Domain. Int J Eng Technol. 2018; 7(3.12): 711-714.
4. Zhao J, Fan Sh, Jia J, Zhang Sh, Jiang B, Xu W, et al. Texture Directionality-Based Digital Watermarking in Nonsubsample Shearlet Domain. Math Probl Eng, 2017; (2017):1-14.
5. Vijay Ananth S, Sudhakar P. Performance Analysis of a Combined Cryptographic and Steganographic Method over Thermal Images using Barcode Encoder. Indian J. Sci. Technol. 2016; 9(7): 1-5.
6. Subhedara MS, Mankar VH. Current status and key issues in image steganography: A survey. Comput Sci Rev. 2014; (13-14): 95-113.
7. Li B, He JH, Huang JW, Shi YQ. A Survey on Image Steganography and Steganalysis. JIHMSP. 2011; 2(2): 142-173.
8. Laishram D, Tuithung TH. A Survey on Digital Image Steganography: Current Trends and Challenges, Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT) Jaipur, India. 2018: 1-17.
9. Sun Sh, Guo Y. A Novel Image Steganography Based on Contourlet Transform and Hill Cipher. JIHMSP. 2015; 6(5): 889-897.
10. Taha MS, Mohd Rahim MS, Lafta SA, Hashim MM, Alzuabidi HM. Combination of Steganography and Cryptography: A short Survey, 2nd International Conference on Sustainable Engineering Techniques (ICSET 2019). Baghdad, Iraq. IOP Conf Ser Mater Sci Eng. 2019; (518): 1-14.
11. Sun Sh. A New Information Hiding Method Based on Improved BPCS Steganography. Adv. Multimed. 2015; (2015): 1-7.
12. Ahmaderaghi B, Kurugollu F, Rincon J, Bouridane A. Blind image watermark detection algorithm based on discrete shearlet transform using statistical decision theory. IEEE Trans Comput Imaging. 2018; 4(1):46-59.
13. Hemalatha S, Dinesh Acharyaa U, Renuka A. Wavelet transform based steganography technique to hide audio signals in image. Procedia Comput Sci. 2015; 47(2015): 272-281.
14. Singh L, Singh AK, Singh PK. Secure data hiding techniques: a survey. Multimed Tools Appl. 2018; 2018:1-21.
15. Hamza YA. Highly Secure Image Steganography Approach Using Arnold's Cat Map and Maximum Image Entropy. Proceedings of the International Conference on Information and Communication Technology ICICT'19, Baghdad, Iraq, ACM. 2019:134-138.
16. Mostaghim M, Boostani R. CVC:Chaotic visual cryptography to enhance steganography. 11th International ISC Conference on Information Security and Cryptology (ISCISC), Tehran, Iran. IEEE. 2014: 44-48.
17. Li Sh, Kang X, Fang L, Hu J, Yin H. Pixel-level image fusion: A survey of the state of the art. Inf Fusion. 2017; 33 (2017): 100-112.
18. Kutyniok G, Labate D. Introduction to Shearlets. Shearlets: Multiscale analysis for multivariate data. In: Kutyniok G, Labate D, editors. Applied and Numerical Harmonic Analysis. Boston: Birkhäuser Basel; 2012. Chapter (1).
19. Moonon A, Hu J, Li SH. Remote Sensing Image Fusion Method Based on Nonsubsampled Shearlet Transform and Sparse Representation. Sens Imaging. 2015; 16(23): 1-18.
20. Naor M, Shamir A. Visual Cryptography. Proceedings of the Advances in Cryptology, Perugia, Italy, EUROCRYPT'94 Springer. 1994; 950: 1-12.
21. Dahata AV, Chavan PV. Secret Sharing Based Visual Cryptography Scheme Using CMY Color Space. International Conference on Information Security & Privacy (ICISP2015), Nagpur, India. Procedia Comput Sci. 2015; 78 (2016): 563-570.

Open Access **Baghdad Science Journal** **P-ISSN: 2078-8665**
Published Online First: July 2021 **2022, 19(1): 197-207** **E-ISSN: 2411-7986**

طريقة محسنة لاخفاء المعلومات في الصور باستخدام تحويل Shearlet المتقطع والمشاركة السرية

ياسر احمد حمزة[1] **ندى ايليا توفيق[1]** **محمد قاسم احمد[2]**

[1]قسم علوم الحاسبات، كلية الحاسبات وتكنولوجيا المعلومات، جامعة نوروز، دهوك، العراق
[2]قسم علوم الحاسبات، كلية التربية، جامعة الحمدانية، الموصل- العراق

الخلاصة:

في الآونة الأخيرة، جعل الإنترنت المستخدمين قادرين على نقل الوسائط الرقمية بطريقة أسهل. على الرغم من هذه السهولة للإنترنت، إلا أنه قد تؤدي إلى العديد من التهديدات التي تتعلق بسرية محتويات الوسائط المنقولة مثل مصادقة الوسائط والتحقق من تكاملها. لهذه الأسباب ، يتم استخدام أساليب إخفاء البيانات والتشفير لحماية محتويات الوسائط الرقمية. فى هذه الورقة البحثية ، تم اقتراح طريقة معززة لإخفاء المعلومات بالصور مع التشفير المرئي. يتم تشفير الشعار السري (صورة ثنائية) بالحجم (128 × 128) عن طريق تطبيق التشفير البصري (2 out 2 share) لتوليد مشاركتين سريتين. أثناء عملية التضمين ، يتم تقسيم الصورة غطاء RGB بحجم (512 × 512) إلى ثلاث طبقات (الأحمر والأخضر والأزرق). يتم تحويل الطبقة الزرقاء باستخدام التحويل Shearlet المتقطع للحصول على معاملاتها. يتم تضمين المشاركة السرية الأولى في معاملات الطبقة الزرقاء المحولة للحصول على صورة الاخفاء. في عملية الاستخراج ، يتم استخراج المشاركة السرية الأولى من معاملات الطبقة الزرقاء لصورة الاخفاء وثم يتم تطبيق عملية XOR عليها مع المشاركة السرية الثانية لإنشاء الشعار السري الأصلي. وفقًا للنتائج التجريبية ، فإن الطريقة المقترحة قد حققت افضل نسبة من عدم الوضوح لصورة الاخفاء بقدرة الحمولة الصافية تساوي (1 bpp). أصبح الشعار السري أكثر أمانًا باستخدام التشفير المرئي (2 out 2 share) والمشاركة السرية الثانية كمفتاح خاص ايضاً.

الكلمات المفتاحية: الطبقة الزرقاء، تحويل Shearlet المتقطع، اخفاء المعلومات في الصور، صورة الاخفاء، المشاركة السرية.