ESTEEM Academic Journal
Vol. 15, June 2019, 44-55

Modified Algorithm for Image Watermarking using 2D-DCT and Elgamal Cryptosystem

Nur Azien Yazid[1], Kamilah Abdullah[1] and Suhaila Abd Halim[1]
[1]*Centre of Mathematics Studies, Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA 40450 Shah Alam. Malaysia*
**corresponding author: [1]kamilah@fskm.uitm.edu.my*

ARTICLE HISTORY

Received
15 April 2019

Accepted
18 June 2019

Available online
30 June 2019

ABSTRACT

Image watermarking embeds identifying information in an image in such a manner that it cannot easily be removed. For the past several years, image digital watermarking has become a necessary element used for hid ing secret image and enabling secured communication such as privacy, confidentiality, authentication and data integrity. Although numerous watermarking schemes are present in grayscale images, the present work focuses on the RGB color image. This study proposed a new hybrid method that would satisfy the essential needs of modern image watermarking. The color image watermarking is based on the 2D Discrete Cosine Transform and Egamal cryptosystem.The 2D Discrete Cosine Transform depends on the matrix products, while the ElGamal cryptosystem depends on the discrete logarithm problem. The cryptosystem is combined with existing Arnold transform in watermarking algorithm to enhance the security of secret image. Value of Peak Signal to Noise Ratio was taken as performance evaluation parameters. On the whole, the performance evaluation shows that combining the two algorithms improved the performance of image watermarking.

Keywords: *Image watermarking; 2D Discrete Cosine Transform; ElGamal cryptosystem; Arnold transform; Peak Signal to Noise Ratio.*

1. INTRODUCTION

At present, more digital information and digital data are being transmitted as compared to a few years ago. A lot of applications were involved in the process of transmitting the data, namely in the fields of education, entertainment, media, medicine and the military. These applications have revolutionized the way digital images, video and audio can be captured, stored, transmitted and manipulated [1].

Digital watermarking can be used to detect images that have been illegally distributed. There are two major process in digital watermarking process namely the embedding process and the extraction process. In the embedding process, the watermark is inserted into an original image, while in the extraction process the watermark is pulled out from an original image [2].

In general, there are two domains for embedding watermarking scheme which are; spatial and frequency [1-6]. In spatial domain, the pixels in original image can be replaced with the pixels in the watermarked image [7-8]. While in frequency domain, the coefficients of a transformed

p-ISSN 1675-7939; e-ISSN 2289-4934

image can be replaced with the pixels of watermarked image [9-10]. However for spatial domain, the program on the sophisticated computer can easily discover the inserted watermark. In the frequency domain, some transformations like Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT) and Discrete Fourier Transform (DFT) are commonly used [11].

Besides, there are three categories in watermarking scheme based on user's embedding process which are robust, semi-fragile and fragile. Robust watermarks are against arbitrary and vicious attacks such as image scaling, bending, cropping and lossy compression [8][10][12]. While semi-fragile is designed to detect any unauthorized modification and allow the image processing at the same time [13] and fragile watermarks are adopted to discover any unauthorized changes for the purpose of image authentication [14][15][16][17][18].

Digital watermarking is important to maintain the security of private image from any interference by the third party. General process of digital watermarking involves inserting the information into a cover image. If the information is too dark or large, it can be focussed by the viewer. This enables the viewer to defuse and alter the information.

Shashank et al. (2016)[19] proposed a color image watermarking using combination of DWT and RSA cryptosystem. According to the proposed scheme, the Peak Signal to Noise Ration (PSNR) value for Lena color image is quite low which is 43.291dB. The performance evaluation shows that the proposed scheme performs a low value PSNR as compared to the watermarked image.

The main goal of this paper is to propose watermarking algorithm with good quality colors for watermarked image. Hence the following objectives have been set up in order to implement embedding and extration algorithms for digital color image watermarking using combination of 2D-DCT and ElGamal cryptosystem, to scramble the secret image by using Arnold transform and to apply inverse 2D-DCT to reconstruct the watermarked image.

2. LITERATURE REVIEW

There are several research related to this work. In this section, the reviewed literatures were written down and used as references and guidelines to develop this study.

2.1 2D Discrete Transform

2D discrete cosine transform (2D-DCT) is a mathematical form that can be transformed from each pixel of an image in the spatial domain into the frequency domain of DCT coefficient. According to [21], 2D-DCT is one of the methods to transform spatial domain to frequency domain. The coefficients can be divided into three different frequencies which are high, middle and low frequency bands by using a zigzag scan. The embedding process of watermark usually occurs in the middle frequency (7-28 coefficients) because the low frequency band has the most energy. This is because low bands are perceptually significant portion of an image, while the high frequency bands are vulnerable to attacks [22]. Nowadays, many researchers have enhanced and hybrid the method of DCT in watermarking.

As mentioned by [22], Fast Discrete Curvelet Transform and Discrete Cosine Transform (FDCuT-DCT) watermarking that are applied in the medical images do not only help to secure the images from being corrupted by eavasdropper but they also help the patients from getting a wrong diagnosis from doctors.

Shih (2007) [2] found that 2D discrete cosine transform (2D-DCT) was provided from a real part of Fourier series. If $f(x,y)$ denotes as an image in spatial domain and $F(u,v)$ denotes an image in frequency image, then the general equation of 2D-DCT is [2]:

$$\mathrm{F}(u,v) = C(u)C(v)\sum_{x=0}^{N-1}\sum_{y=0}^{N-1} f(x,y)\, cos\left(\frac{(2x+1)u\pi}{2N}\right) cos\left(\frac{(2y+1)v\pi}{2N}\right)$$

where if $u = v = 0, C(u) = C(v) = \sqrt{\frac{1}{N}}$; otherwise, $C(u) = C(v) = \sqrt{\frac{2}{N}}$

The inverse DCT can be represented as

$$\mathrm{f}(x,y) = \sum_{u=0}^{N-1}\sum_{v=0}^{N-1} C(u)C(v)F(u,v)\, cos\left(\frac{(2x+1)u\pi}{2N}\right) cos\left(\frac{(2y+1)v\pi}{2N}\right)$$

2.2 ELGamal Cryptosystem

In ElGamal cryptosystem, the underlying mathematical relationship between the encryption and decryption keys relies upon the discrete logarithm problem [23]. In this system it is fundamental to have the knowledge of the secret key to make the decryption easier. However, if the private key is unknown, it is nearly impossible to decrypt the message even in.

Due to our country's progressions, many organizations, companies, government's agencies as well as individuals are using cryptography techniques in order to ensure the safety of the communication and the exchange of information. This is why ElGamal cryptosystem is widely used in the communication authentication and privacy guard software such as GNU privacy guard as a standard practice for signatures [24]. In addition Tsiounis and Yung (1998) [25] have also discussed the decision of Diffie-Hellman's assumption in their paper. This assumption was based on the original ElGamal cryptosystem without any modification. The semantic security of the ElGamal encryption is equal to the decision of the Diffie-Hellman problems. This is shown by reducing some sub-protocols.

A recent alternative method to group encodings and hash function was introduced in the paper by Chevallier-Mames et al. (2006) [26]. To embed the message into a group element that consists in converting the session key output by the Diffie-Hellman key exchange into an integer modulo p using the class function. The cryptosystem featured is better than the original ElGamal cryptosystem and remain comparable in computation speed.

Kiltz and Pietrzak (2010) [27] supported the use of public key cryptosystem against side channel attack by using the blinding method. This method was used to arbitrary an exponentiation in sequence to prohibit multiple measurements of the same operation on different data. Since the development of the ElGamal cryptosystem, there are so many algorithms constructed to attack and solve the discrete logarithm of small size numbers like Baby Step Giant Step algorithm and Pollard's rho algorithm [28].

Sharma et al. (2012) [29] proposed an intensified ElGamal cryptosystem to improve the security for encrypting long messages and defend mathematical and brute force attack securely. The difficulty in solving the discrete logarithm problem and integer factorization problem influence the security of the algorithm. The combination of factorization of large number and the discrete logarithm problem is the core of the intensified ElGamal cryptosystem. However, the enhanced security is a trade off to the speed of computation process of the newly proposed cryptosystem as more time is required for the encryption process.

To encrypt large messages, ElGamal scheme needs to be improved to be more efficient than before. The adversary has no ability to obtain any information about the plaintext, is a proof that the ElGamal Public Key Encryption (ElGamal PK) is secured in perceiving the Indistinguishability Adaptive Chosen-Cipher Text Attack (IND-CCA2). Although the efficiency of ElGamal PKE is well recognized, its effectiveness to encrypt large messages is still being disputed. [30].

Jing et al. (2012) [31] proposed a new type of ElGamal public key cryptosystem based on ergodic matrix. This technique is not easy to handle in a standard model like polynomial discrete logarithm problem over finite field. It is exposed to attack by linear equation that has a higher level order. The security level is quite similar to the original ElGamal scheme.

2.3 Arnold Transform

Arnold transform is one of the methods for scrambling technique that can make a security level to become better and is applied before watermarked embedding. This has been proven by [35] that obtained better invisibility and robust under some attacks.

The process of image will be brought to its original state after the multiple iterations by virtue of this transform. The 'Arnold Period' or 'Periodicity of Arnold Transform' is terms for the number of iterations. The Arnold transform can be represented as [32]:

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} (\text{mod } N) \qquad (3.3)$$

where (x, y) is the pixel coordinates of the original image and (x', y') is the pixel coordinates of the scrambled image [19].

This transformation is called two-dimensional Arnold scrambling. For $x, y \in \{0, 1, 2, 3, \ldots, N - 1\}$, N is represented as the order of digital image matrix. Considering the feedback, $(x, y)^{\mathrm{T}}$ is the input in the right while $(x', y')^{\mathrm{T}}$ in the left is the output, in which the iterative process can be represented as the following [32]:

$$P_{xy}^{n+1} = AP_{xy}^{n} (\text{mod } N) \qquad (3.4)$$

$$P_{xy}^{n} = (x,y)^{\mathrm{T}} \qquad (3.5)$$

where n represented as the time of iterations which $n = 0, 1, 2, \ldots..$

After all of the points of the original image have been traversed, these will then generate a new image. In addition, the Arnold scrambling also has the cycle character. Table 1 shows the algorithm cycling of Arnold transform with different sizes of images.

Table 1: *Arnold transform Algorithm Cycle [32]*

Size of image (*N*)	Cycle of scrambling (*T*)	Size of image (*N*)	Cycle of scrambling (*T*)
3	4	25	50
4	3	32	24
5	10	64	49
6	12	100	150
7	8	120	60

To descramble the scrambled image, the inverse matrix from equation (3.3) needs to be applied to the scrambled image. In this process, the pixel coordinate (*x', y'*) will be repositioned (*x, y*), so the original image will be displayed

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} (\text{mod } N) \qquad (3.6)$$

where (*x', y'*) is the pixel coordinates of scrambled image and (*x, y*) is the pixel coordinates of the original image.

Even though many methods have been applied in image watermarking, these methods are still lacking in terms of encryption and decryption of the messages. Thus, this project aims to improve the number of PSNR value which illustrates the security level of the watermarking that is combined with the algorithm to encrypt and decrypt the messages.

3. METHODOLOGY

This study presents a color image watermarking based on 2D-DCT to transform the original cover image and ElGamal cryptosystem to encrypt the secret image before being embedded into the transformed cover image. Additionally, ElGamal algorithm is used to improve the security of the scheme. Besides that, Arnold Transform is also used for scrambling the secret image before encrypting. The whole implementation of the algorithms was implemented using MATLAB R2016a.

3.1 Embedding Process

Embedding is one of the main processes in digital watermarking scheme. It is not only used in image watermarking, but also in audio or video watermarking process as well. In the embedding process, the secret image is inserted into the cover image. Such a process could be described as follows:

$$E = C + vS \qquad (3.7)$$

where *E* is the embedded image, *C* is the transformed cover image, *S* is the encrypted-scrambled secret image and *v* is a scaling factor, which is set to 0.002. The scaling factor affects the robustness and imperceptibility of the watermarked image [33]. The higher the scaling factors are, the worst the imperceptibility and robustness become. Below is the embedding algorithm that is proposed in this study.

Table 2:Embedding Algorithm with 8x8 2D-DCT with ElGamal Cryptosystem

Step 1: Read the 512 × 512 pixels color of cover image and secret image.
Step 2: Divide the cover image into 8x8 blocks and apply 2D-DCT on each block to transform the cover image.
Step 3: Carry out the Arnold transform on the color secret image to construct scrambled secret image.
Step 4: Encrypt the scrambled secret image using ElGamal cryptosystem.
Step 5: Embed the encrypted-scrambled secret image into transformed cover image to get embedded image.
Step 6: Apply the inverse 2D-DCT on the embedded image and construct the watermarked image.

By using the idea that is proposed in [19], both processes for secret image and cover image occur simultaneously. The secret image is scrambled using Arnold transform and image encryption using Elgamal cryptosystem, while the cover image will go through a transformation process using 2D-DCT. After the image scrambling process is completed, the scrambled secret image will have to go through the encryption process using ElGamal cryptosystem.

To improve the security, both cover and secret images will pass through different processes before committing the embedding process. This is to improve the security in the respective process. Therefore, the images that are used in this study must be in the same size in pixels and format : 512 × 512 and ".jpeg" file, respectively. "Dahlia" is the secret image while baboon, Lena, sea and forest are the cover images. All images can be found on Google Image.

3.2 Extraction Process

The extraction process (inverse of embedding process) requires a watermarked image to extract the secret image and cover image. In this extraction process, there are two processes which are to extract the transformed cover image and encrypted-scrambled secret image. It is described as follows:

i. Transformed cover image

$$C = E - vS \tag{3.8}$$

ii. Encrypted-scrambled secret image

$$S = \frac{(E - C)}{v} \tag{3.9}$$

where E is the embedded image, C is the transformed cover image, S is the encrypted-scrambled secret image and v is a scaling factor, which is set to 0.002 same as in embedding process. For extraction process, the proposed algorithm is as in Table 3.

Table 3:Extraction Algorithm with 8x8 2D-DCT with ElGamal Cryptosystem

Step 1: Input the color watermarked image.
Step 2: Apply back 2D-DCT into the watermarked image to get the embedded image.
Step 3: Extract the embedded image to get the transformed cover image and encrypted-scrambled secret image.
Step 4: Apply inverse 2D-DCT on transformed cover image to construct the extracted cover image.
Step 5: Decrypt the encrypted-scrambled secret image using ElGamal cryptosystem and get the scrambled secret image.
Step 6: Descramble the scrambled secret image using Arnold Transform to obtain the extracted secret image.

Similar to the embedding process, the process on transformed cover image and encrypted-scrambled secret image occur simultaneously [19]. In the part of ElGamal decryption process, the encrypted-scrambled secret image will go through the decryption process that was mentioned earlier. From that process, the scrambled secret image would be constructed.

3.3 Evaluation Process

The performance of watermarked image was evaluated using the Peak Signal to Noise Ratio (PSNR). The PSNR value is the degradation between the original image and watermarked image. The PSNR value is measured in decibles (dB). The higher the PSNR value, the better the watermark conceals. The formula of PSNR value can be represented as (Lin et al., 2012):

$$PSNR = 10\log_{10}\left(\frac{R^2}{MSE}\right) \tag{3.10}$$

where R is the maximum possible pixel value the image. For example, the pixels are represented using 8 bits per sample, this is 255. More generally, when samples with B bits per sample, R is 2^B-1. While by Lin et al. (2012), formula Mean Square Error (MSE) represented as

$$MSE = \frac{\sum_{M,N}[I_1(m,n)-I_2(m,n)]^2}{M*N} \tag{3.11}$$

where $I_1(m,n)$ is the pixel value of cover image, $I_2(m,n)$ is the pixel value of watermarked image then M and N is the number of rows and columns of an input image.

4. RESULTS

The transformation process does not give any effect to the size of image dimension, but it only changes the pixel value of the image which affects its resolution. Figure 1 shows the exchange of 'baboon.jpeg' which is from the original cover image transformed using 2D-DCT.

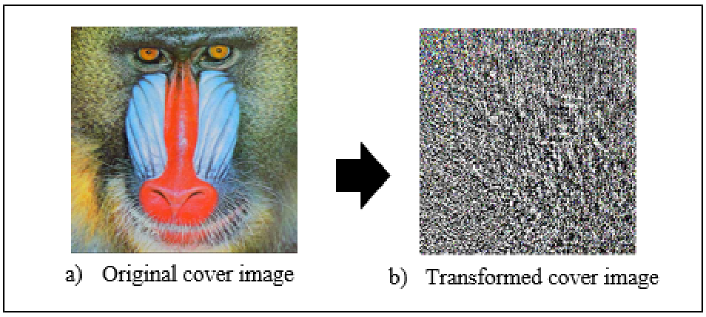


Figure 1: Exchange in 'baboon.jpeg' image a) Original cover image; b) Transformed cover image

This encryption process used one public key that was only known by the sender and another public key known by both the sender and receiver. In this study, the elements of public keys are (3, 131, 257) and the private key used was 7. The exchange of 'dahlia.jpeg' image is shown in Figure 2.

p-ISSN 1675-7939; e-ISSN 2289-4934

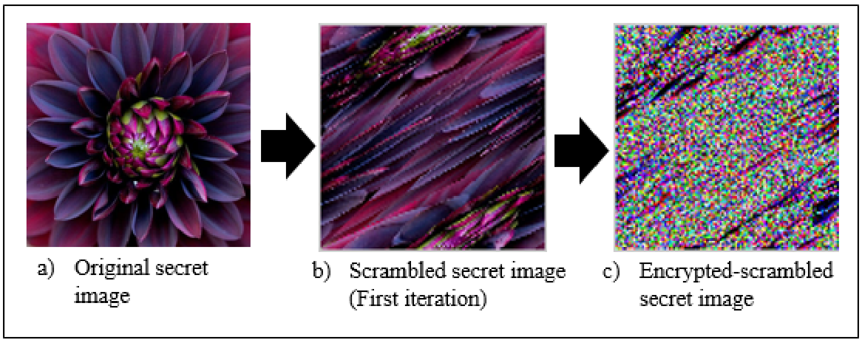

a) Original secret image
b) Scrambled secret image (First iteration)
c) Encrypted-scrambled secret image

Figure 2: Exchange in 'dahlia.jpeg' image a) Original secret image; b) Scrambled secret image (First iteration); c) Encrypted-scrambled secret image

Figure 3 shows the example of the embedding process between the transformed cover image and the encrypted-scrambled secret image. Then, the embedded image was inversed using 2D-DCT to get the watermarked image. This process was done to get the original cover image while removing any transformation in the image.

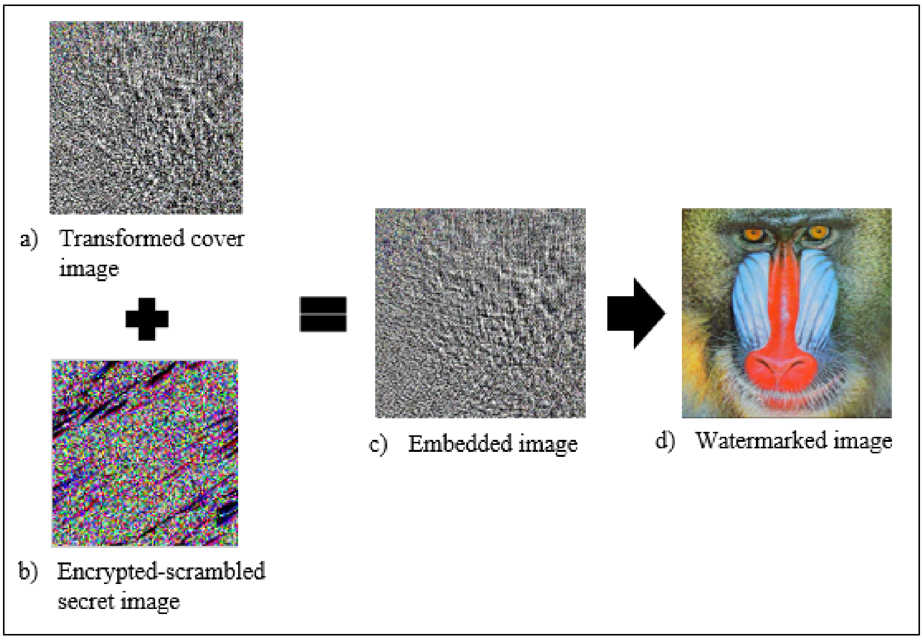

a) Transformed cover image
b) Encrypted-scrambled secret image
c) Embedded image
d) Watermarked image

Figure 3: Example of embedding process between the transformed cover image and the encrypted-scrambled secret image

Figure 4 shows the example of extraction process for the watermarked image 'baboon.jpeg' in order to extract the secret image of the 'dahlia.jpeg'.

p-ISSN 1675-7939; e-ISSN 2289-4934

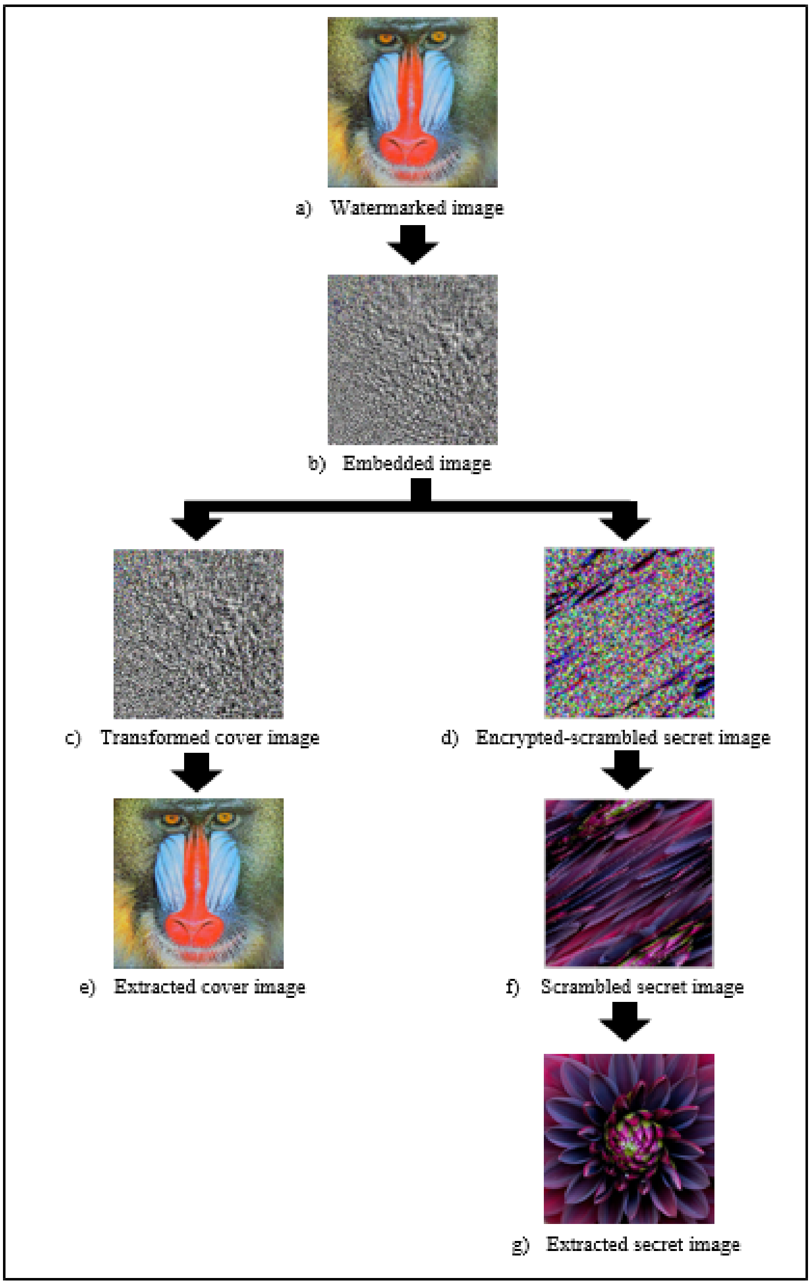
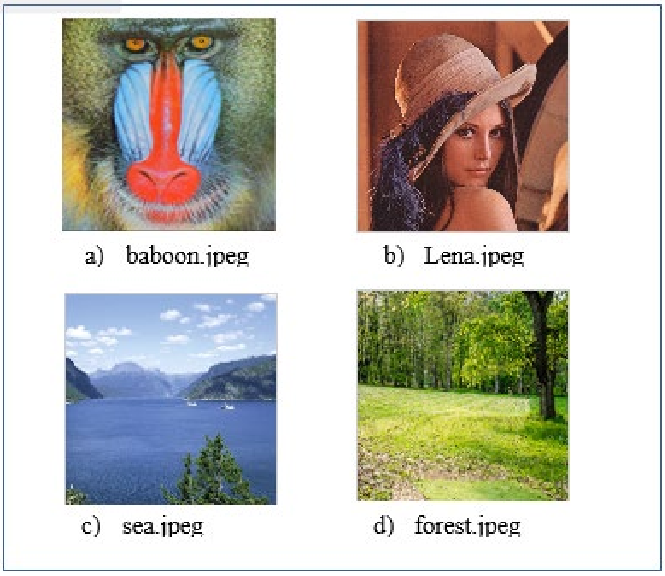

a) Watermarked image
b) Embedded image
c) Transformed cover image
d) Encrypted-scrambled secret image
e) Extracted cover image
f) Scrambled secret image
g) Extracted secret image

Figure 4: Example of extraction process for watermarked image

All cover images were embedded with a secret image ‘dahlia.jpeg’. The processing of Arnold transform and ElGamal cryptosystem were applied to the secret image before it was embedded into the cover image. Thus, every cover image constructed its own watermarked image using the same process as shown in Figure 5. All images were color scale images with 512 × 512 pixels.



a) baboon.jpeg

b) Lena.jpeg

c) sea.jpeg

d) forest.jpeg

Figure 5: The watermarked image

The PSNR value is the degradation between the original image and watermarked image. The PSNR value is measured in decibles (dB). The higher the PSNR value, the better the watermark conceals. Table 3 shows the quality of 4 cover images used in this study to cover the secret image using the embedding algorithm.

Table 3: The PSNR (in dB) values of watermarked image using proposed algorithm

Cover Image	Baboon	Lena	Sea	Forest
PSNR	60.3798	60.8804	61.2944	60.2616

The PSNR values for baboon and forest are lower than original watermarked image because both images have more vivid colours compared to the other two images. Table 4 shows the PSNR of two secret images ('lena.jpeg' and 'baboon.jpeg') as compared to 4 other algorithms proposed by different authors.

Table 4: The PSNR (in dB) values of previous and proposed scheme for Lena and baboon color image

Cover Image	PSNR value (dB)				
	Mohamed et al. Scheme (2015)	Aparna & Sonal Scheme (2015)	Shashank et al. Scheme (2016)	Chang & Tai Scheme (2013)	Proposed Scheme
Lena	73.12	64.13	43.29	44.36	60.88
Baboon	71.48	-	-	-	60.38

5. CONCLUSION

This study proposed a method based on the combination of ElGamal cryptosystem and 2D-DCT. The mathematical problem in ElGamal cryptosystem gives additional difficulties in order to apply it in a secret image. Usually this cryptosystem is applied on secret messages in word or number form. However in this study, some modification was made to the ElGamal cryptosystem to enable this cryptosystem to be applied on an image using the same technique.

Therefore, it can be concluded that the image watermarking scheme that is combined with cryptosystem gives better result than without using any cryptosystem. This is because, the security of the secret image will be less risky when it is encrypted before being embedded into the cover image. However the PSNR value will decrease significantly when the watermarked image is attacked by other forms of attack, such as the contrast attack. Thus, it is clear that that the proposed scheme is less robust than the other methods.

ACKNOWLEDGEMENT

The authors would like to express our gratitude to the Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Shah Alam for the opportunity and technical support in completing this study.

REFERENCES

[1] H. Berghel and L. O'Gorman, "Protecting Ownership Rights through Digital Watermarking," *IEEE Computer Magazine*, 29, 101, 1996.

[2] F. Y. Shih, "Digital Watermarking and Steganography: Fundamentals and Techniques," *CRC Press: Taylor & Francis Group*, 2007.

[3] I. Cox. and M. Miller,. "The First 50 Years of Electronic Watermarking," *Journal of Applied Signal Processing*, vol. 2, pp.126-132, 2002.

[4] I. J. Cox, , J. Kilian, T. Leighton, and T. Shamoon, "Secure Spread Spectrum Watermarking for Multimedia," *IEEE Transactions on Image Processing*, vol. 6, pp. 1673-1687, 1997.

[5] G. C. Langelaar, I. Setyawan, and R. L. Lagendijk, "Watermarking Digital Image and Video Data," *IEEE Signal Processing*, vol. 17, pp. 20-46, 2000.

[6] F. A. P. Petitcolas, R. J. Anderson and M. G. Kuhn, "Information Hiding-A Survey," *Proceeding of the IEEE*, vol. 87, pp. 1062-1078, 1999.

[7] O. Bruyndonckx, J. J. Quisquater and B. Macq, "Spatial Method for Copyright Labeling of Digital Images," *Proceedings IEEE Workshop Nonlinear Signal and Image Processing*, 1995.

[8] A. Dixit and R. Dixit, "A Review on Digital Image Watermarking Techniques," *International Journal Image, Graphics and Signal Processing,* vol. 4, pp. 56-66, 2017.

[9] J. Huang, Y. Q. Shi and Y. Shi, "Embedding Image Watermarks in DC Components," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 10, pp. 974-979, 2000.

[10] S. D. Lin and C. F. Chen, "A Robust DCT-Based Watermarking for Copyright Protection," *IEEE Transactions Consumer Electronics*, vol. 46, pp. 10-11, 2000.

[11] K. Mahmoud, S. Datta and J. Flint, "Frequency Domain Watermarking: An Overview," *The International Arab Journal of Information Technology*, vol. 2 no. 1, pp.33-47, 2005.

[12] U. Yadav, J. P. Sharma, D. Sharma and P. K. Sharma, " Different Watermarking Techniques & It's Application: A Review," *Int. Jour. of Scientific & Engineering Research,* vol. 4, issue 4, pp. 1288-1294, 2014.

[13] X. Yu, C. Wang and X. Zhou, " Review on Semi-Fragile Watermarking Algorithms for Content Authentication of Digital Images," Future Internet, vol. 9, 2017.

[14] C. Qin, P. Ji, J. Wei and C. C. Chang, "Fragile image watermarking scheme based on VQ index sharing and self-embedding," *Mulimedia Tools and Applications,* vol. 76, pp. 2267-2287, 2017.

[15] M. U. Celik, G. Sharma, E. Saber and A. M. Tekalp, "Hierarchical Watermarking for Secure Image Authentication with Localization," *IEEE Transactions on Image Processing*, vol. 11, pp. 585-595, 2002.

[16] C. Qin, P. Ji, X. Zhang, J. Dong and J. Wang, " Fragile image watermarking with pixel-wise recovery based on overlapping embedding strategy," *Journal of Signal Processing,* pp. 280-293, 2017.

[17] A. Shehab, M. Elhoseny, K. Muhammad and A. K. Sangaiah, P. Yang, H. Huang and G. Hou, "Secure and Robust Fragile Watermarking Scheme for Medical Images," *Soft Computing Tech. For Image Analysis in the Medical Industry,* vol. 6, 2018.

[18] C. Wang, H. Zhang and X. Zhou, " A Self-Recovery Fragile Image Watermarking with Variable Watermark Capacity," *Applied Sciences,* vol. 8, pp. 548, 2018.

[19] M. R. Shashank, R. Srujan, V. Madhukar, H. S. Rahul and K. V. Sandeep, "A Secure Color Image Watermarking Scheme Using RSA Encryption," *International Journal of Engineering Science and Computing*, vol. 6, no. 5, pp. 4948-4950, 2016.

[20] M.Moosazadeh and G. Ekbatanifard, "An Improved Robust Image Watermarking Method Using DCT and YCoCg-R Color Space," *Optik 140*, pp. 975-988, 2017.

[21] M.Khalili, "DCT-Arnold Chaotic Based Watermarking Using JPEG-YcbCr," *Optik,* vol. 126, no. 23, pp. 4367-4371, 2015.

[22] R. Thanki, S. Borra, V. Dwivedi and K. Borisagar, "An Efficient Medical Image Watermarking Scheme Based On FDCuT-DCT," *International Journal Engineering Science and Technology*, vol. 20, pp. 1366-1379, 2017.

[23] A. V. Meier, "The ElGamal Cryptosystem," *Joint Advanced Students Seminar 2005,* pp. 1-13, 2005.

[24] P. K.Arya, M. S. Aswal and V. Kumar, "Comparative Study of Asymmetric Key Cryptographic Algorithms," *International Journal of Computer Science & Communication Networks,* vol. 5, no. 1, pp. 17-21, 2012.

[25] Y. Tsiounis and M. Yung, "On the Security of ElGamal Based Encryption," *Springer-Verlag Berlin Heidelberg,* pp. 117-134, 1998.

[26] B. Chevallier-Mames, P. Paillier and D. Pointcheval, "Encoding-Free ElGamal Encryption Without Random Oracles," *International Workshop on Public Key Cryptography,* pp. 91-104, (2006).

[27] E. Kiltz, and K. Pietrzak, "Leakage Resilient ElGamal Encryption," *Advances in Cryptology-ASIACRYPT 2010*, pp. 595-612, 2010.

[28] K. Rabah, "Security of the Cryptographic Protocols Based on Discrete Logarithm Problem," *Journal of Applied Sciences,* vol. 5, pp. 1692-1712, 2005.

[29] P. Sharma, A. K. Gupta and S. Sharma, "Intensified ElGamal Cryptosystem," *International Journal of Advances in Engineering & Technology,* vol. 2, no. 1, pp.543-551, 2012.

[30] T. Y.Chang, M. S. Hwang and W. P. Yang, "Cryptanalysis on an Improved Version of ElGamal-like Public-Key Encryption Scheme for Encrypting Large Messages," *Informatica Vilnius University,* vol. 23, no. 4, pp. 537-562, 2012.

[31] Z. J. Jing, G. P. Jiang and C. S. Gu, "A Novel Public Key Cryptosystem Based on Ergodic Matrix over GF(2)," *IEEE Computer Society,* pp. 845-848, 2012.

[32] M. Li, T. Liang and Y. J. He, "Arnold Transform Based Image Scrambling Method," *Atlantis Press,* pp. 1309-1316, 2013.

[33] G. Pavel, "Embedding, Extraction and Detection of Digital Watermark in Spectral Images," *Lappeenranta University of Technology*, 2005.

[34] G. Lin, G. Tiegang, S. Guorui, C.Yanjun, & F. Li, "A New Reversible Watermarking Scheme Based on Integer DCT for Medical Images". *Proceedings of the 2012 International Conference on Wavelet Analysis and Pattern Recognition*, 33-37, 2012.

[35] Z. Zhang, C. Wang and X. Zhou, " Image watermarking scheme based on Arnorld transform and DWT-DCT-SVD". *Internation Conference on Signal Processing (ICSP),* pp. 805-810, 2016.