DOI: https://doi.org/10.33103/uot.ijccce.22.1.5

Holographic Digital Image Watermarking Based on Chaos Techniques

Donya Y. Abdulhussain[1], Hala Bahjat AbdulWahab[2],
Abdulmohsen jaber Abdulhoseen[3]
[1,2]*Department of Computer Science, University of Technology, Baghdad, Iraq*
[3]*Turath University college, Baghdad, Iraq*
[1]donya95y@gmail.com, [2]110005@uotechnology.edu.iq, [3]Abdulmohsen.jaber@turath.edu.iq

Abstract— *Digitally, a large number of information was generated, stored and exchanged. This growth leads to problems that needed to solve. Digital watermarking has been one of the key terms to secure and authenticate the owner's information.*

The watermarking image technology is a procedure for embedding secret data into an original image. In this paper, encrypted holographic watermark image was proposed by using chaotic technique, which utilizing three distinct chaos maps: logistic, Arnold and Baker; to ensure the security to the system.

Performance evaluation of embedding and decrypted Watermark image measured by Peak to signal ratio (PSNR), Structural Similarity (SSIM), Mean square error (MSE), Root mean square (RMSE), and Normalize Root mean square (NRMSE).

Results and outcomes of measurements confirmed the robustness of the chaotic technique and also the Histogram showed the good distribution of the encrypted holographic image pixels and observed that the encrypted holographic image in bit are significantly uniform and different from that of the Watermark image that mean the encryption image in bit interleaver is change the level values and position of pixel and also good similarity SSIM about 0.9 for both test 1 and 2.

Index Terms— *Arnold cat map, Baker map, Digital watermark image, Holographic image, Logistic map.*

I. INTRODUCTION

The ultimate objective of a digital watermarking system is to protect data ownership in the original data (image, audio, text or video). It is easier to reproduce the contents of a legal owner without permission from technological development. The reasons for this lie in information about the methods of image processing and internet manipulation open to unauthorized parties. Many researchers worldwide already have suggested various types of efficient watermarking schemes in order to avoid these illegal acts, but at the same time they could hardly guarantee both imperceptibility and power. between the two main properties of an efficient watermarking scheme, the first one is imperceptibility [1].

Imperceptibility means in the host image or cover image that the watermark image or the data should not be visible. The second property is robustness. The hidden watermark image must withstand attacks such as noise, filtering, cutting and rotation. During the design process, the user must compromise these two properties. All watermarking techniques are divided into two groups, namely spatial domain techniques and domain transfer techniques [2,3].

The pixel intensity value in the spatial domain is changed for digital images, but watermarking is not robust in this domain. The digital image coefficients are modulated

Received 21/June/2021; Accepted 22/September/2021
© 2017 University of Technology, Iraq *ISSN (Print) 1811-9212* *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.22.1.5

accordingly in the frequency domain by adding additional data and schema, which is increasingly imperceptible [4].

Over the last few years, optical holography technologies for data protection and digital watermarks have been developed and have shown considerable promise. The holographic optical method will provide us with a number of encoded degrees of freedom, e.g. phase, amplitude, distance of diffraction and wavelength. And this method has many benefits including high design freedom, high strength, tearing difficulty, natural parallelism, and cracking difficulty. Thus, in the area of hiding and digital watermarking, digital holography has a great application prospect [5].

Image security has become an important problem in network communication and encryption is one of ways to ensure digital images safe. Image encryption methods attempt to transform the original image to a different one that is difficult for anyone to understand, with the exception of those who have special expertise and, in other words, no one should know what the information is without a decryption key [6, 7].

Many systems of chaotic image encryption have been suggested, chaotic maps have all the characteristics and specifications of the system to be chaotic, like sensitivity to initial conditions, randomness,and unpredictable, etc., This makes chaotic maps for cryptographic algorithms to be the best choice.

In this research paper, presented a method of digital watermarking that uses holography logo image and encrypted it by chaotic maps and then embed it into an image to construct a watermarked image. The hidden image can be recovered by inverse of chaos encryption and embedding process. chaotic logistic mapping was used to encrypt the holographic logo image Compared with chaotic Arnold mapping and Baker map.

The remainder of this article is organized as follows: In Section II, Literature review are briefly described. Holographic Image in section III, chaos encryption technique with 3 different chaotic maps which used in this research were explained with it's mathmatecal equations in a short way in section IV. The proposed method, including embedding and extraction steps of the watermark in Section V. Section VI presents the experimental results and performance analysis. The conclusions are presented in the end of the paper.

II. LITERATURE REVIEW

In **2015,** Ruichen Jin et al. [8], watermarking technique based on Radon transform that is rotation-invariant. The Radon transform's translation feature is used to produce rotation invariance. Holograms are altered using a Discrete Fractional Random Transform (DFRT) algorithm (DFRNT). Incorporated into an iDWT after being transformed by it. Due to the fact that we do not require the original image for detection, this approach is categorized as a blind watermark. To counter rotational assaults, the suggested approach is resilient.

In **2016,** Li Wang et al. [9], proposed holographic watermark with a fast Fourier method of the Fresnel integral transform (S-FFT). However, it is crucial to note that, by using a four-step phase-shifting method, four images are obtain, and then randomly select one of them to be embedded in the digital watermarking technology of holographic images, with the remaining three holograms being used to store the watermarking information in the optical code.

In **2018,** Xiao Zhou I et al. [10], The APDCBT was incorporated into the hybrid watermarking approach by merging it with DWT and SVD, resulting in a very resilient watermarking algorithm. Experiments have shown that the suggested technique has no influence on the original image and is more resistant to conventional signal processing assaults than previous algorithms.

Received 21/June/2021; Accepted 22/September/2021
© 2017 University of Technology, Iraq ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.1.5

In **2019,** S K Li et al. [11], Presented a novel approach for embedding colored watermarks into carrier images using an algorithm called DCT-DWT (Discrete Cosine Transform - Discrete Wavelet Transform). In place of the original image of the watermark, a holographic watermark is used. To create the hologram, a four-step phase-shift technique is used for each channel's watermark picture to construct it. Experiments have shown that the method is able to withstand conventional assaults while preserving key characteristics of the watermarking.
In **2020,** Zhiyue Liu et al. [12], Watermarking is used in this article in conjunction with DWT-DCT technology, and proposes a digital holographic watermarking algorithm based on the DWT-DCT transform domain, which makes the watermark very invisble and secure. The findings demonstrate that this method is resistant to basic linear assaults as well as noisy attacks, proving its robustness.

III. HOLOGRAPHIC IMAGE

Fourier Transformation help us out to generate holography logo image, we used Fast Fourier Transform (FFT), We can utilize Fourier Transformation to transform our image information - gray scaled pixels into frequencies and do further process. Fast Fourier Transform (FFT) is an algorithm for computing the Discrete Fourier Transform (DFT) in a way that minimize this complexity by a strategy called divide and conquer because of this the computation complexity will be reduced to O(N log N). The FFT is a key image processing method used to break down an image into its frequency components. Two elements, sine and cosine, will be present in the FFT results. A complex number consisting of a real part and an imaginary component is another way to look at this. The transformation input image represents the spatial domain equivalent, while the output represents the image in the Fourier or frequency domain [13].

The FFT magnitude is essentially the amplitude of the frequency variable associated with it. The word magnitude normally means the square root of the squares of both the real (sine) part and the imaginary (cosine) part. The Fourier Transform also only shows the magnitude as it includes most detail about the spatial domain image geometric structure, amplitude varies drastically in images at the edge, or sounds. We can therefore assume that edges and sounds are high frequency in the image. It is a low-frequency component if there are no many changes in amplitude. The outcome shows that the image has components of all frequencies, but for higher frequencies its magnitude becomes smaller. Low frequencies therefore provide more information on the image than higher frequencies. The transformed image also tells us that in the Fourier image, one goes vertically and one crosses the middle horizontally. These come from the standard patterns in the original image background [14].

Digital holographic techniques make it possible to recover the mark with a Fourier transform and to alter the content image and watermark it with the same pattern. After inserting the watermark, the chaos technique is used to improve the safety level of the watermarked image.

IV. CHAOS BASED ENCRYPTION TECHNIQUE

The discovery of chaos theory was made in the early 60s by Edward Lorenz when he creates a weather simulation and describes his sensitivity towards the initial values to show that a small change could lead to enormous differences and be characterized by what is known as a (butterfly) effect [15, 16]. Chaotic maps are mathematical equations which generate random sequences that are extremely sensitive to the parameters of their initial

Received 21/June/2021; Accepted 22/September/2021
© 2017 University of Technology, Iraq ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.1.5

condition and control. Dimensional (1D) and multidimensional (MD) chaotic maps are divided into 2 groups [17].

The fundamental approach to crypto systems focused on chaos includes two phases of operations: confusion and diffusion. First Step is called the pixel permutation or phase of confusion . In this step, the pixel positions over the entire image are modified to make the image unknown. Often this method is called pixel scrambling. The first conditions and control parameters of the chaotic maps are set by scrambling, and the scrambling is iterated several times. However, The image is nevertheless unrecognizable. It is not secure to have only the confusion process because they are susceptible to most attacks. In addition, over the second step known as the diffusion stage, the scraped image is passed on. This procedure aims at changing the pixel value in the image. The adjustment in the pixel value can be made using a chaotic map using the main key of the initial conditions and the control parameters. The pixel value change is reflected in step 1. The chaotic maps are more randomly suited for image encryption [18].

In the next section will review mathematical equations and the behavior of different chaotic maps which are recently used in image encryption research.

A. Logistic map

The logistic map is a polynomial grade 2 mapping. The map has been popularized by biologist Robert May in a seminal paper in 1976. Mathematically, the logistic map is written as: [19]

$$X_{(n+1)} = \mu\, X_{(n)}\,(1 - X_{(n)}) \tag{1}$$

Where n= 0, 1, 2, 3, ... , The parameter μ the reproduction rate, positive parameter $0 < \mu < 4$. $X_{(0)}$ is a number between zero and one that represents the ratio of existing population to the maximum possible population, starting value $0 \leq X_0 \leq 1$ and a the map produces a sequence of values $X_0, X_1, X_2, \ldots$.

The following behaviors are observed by changing the system parameter μ (as *Fig. 1*):

- When the value of μ is between 0 and 1, the iterative values that are sovereign to the initial conditions eventually die.
- If the value of μ is 2 to 3, the iterative value oscillates around a value first and only stabilizes at the same value at long last.
- The iterative values oscillate between two μ values, which depend on μ, if μ is between 3 and 3.45 (around).
- The iterative values oscillating between four values while the μ value is between 3.45 and 3.56 (approximately). This logistical map becomes a chaotic map as the μ value is greater than or equal to 3.57, as a small change in initial state results, over time, in radically different iterative values [19].

Received 21/June/2021; Accepted 22/September/2021
© 2017 University of Technology, Iraq ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.1.5

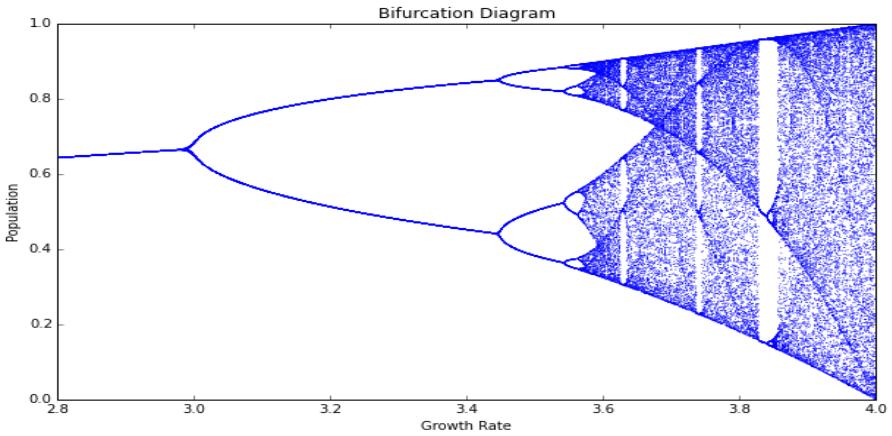


FIG. 1. BIFURCATION DIAGRAM FOR LOGISTIC MAP.

B. Arnold cat map

The Russian mathematician Vladimir Arnold discovered Arnold's Cat map in 1960. Arnold's Cat Map written by the following equation:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} 1 & p \\ q & pq+1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} mod\ n \tag{2}$$

Where p and q are positive integers, the determinant (A) = 1. (x ', y') is the new position of the original pixel position (x, y) when Arnold's Cat Map (ACM) algorithm performed once. The output following the use of the ACM to the number of iterations R is a random drawing with all the values of the same pixel of the image. The number of iterations R to be completed according to the p, q and N image size parameters. therefore, there are parameters p, q and the number of Iterations R in ACM algorithm, all of which can be utilized as a secret key [20].

C. Baker map

As an encryption method, the chaotic Baker map is popular for image processing. It is a permutation-driven tool that randomizes a N x N square matrix by changing the location of the pixels on the basis of a secret key. The pixel is assigned in a bijective way to a different pixel location. The discretized Baker map is an effective method to randomize the objects in a square matrix [21]. Ni = n1+ . . . , + ni−1. The data item at the indices (r, s), is moved to the indices:

$$B(r,s) = \left[\frac{N}{n_i}(r - N_i) + s\ mod\left(\frac{N}{n_i}\right), \frac{n_i}{N}(s - s\ mod\ \left(\frac{N}{n_i}\right)) + N_i\right] \tag{3}$$

Where Ni ≤ r < Ni+ni, 0 ≤ S < N, and N1 = 0. Let B (n1, . . . , nk), denote the discretized map, where the vector, [n1, . . . nk], represents the secret key, Skey . Defining N as the number of data items in one row, the secret key is chosen such that each integer ni divides N, and n1+...,+nk = N.

V. PROPOSED SYSTEM

We have proposed an application ability of digital holographic watermarking into image security. The digital holographic watermarking applied onto a gray scale image. Combining the characteristics of Fast Fourier transform to generate holographic image and chaotic technique to encrypt the logo image.

Received 21/June/2021; Accepted 22/September/2021
© 2017 University of Technology, Iraq
ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.1.5

Holographic Digital Image Watermarking based on chaos techniques is proposed, which makes digital watermarking more robust and invisible.

A. Embedding schema

The embedding process of holographic watermark, the implementation process is shown in *Fig. 2* below:

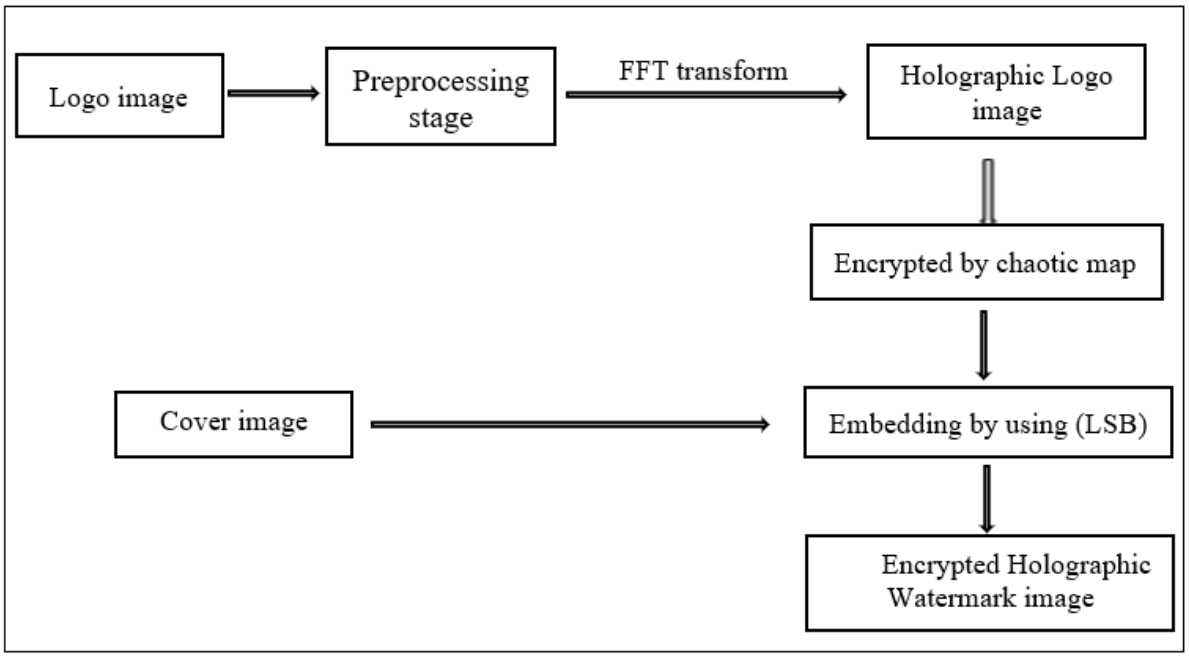


FIG. 2. SCHEMATIC DIAGRAM OF THE PROPOSED SYSTEM (WATERMARK EMBEDDING PROCESS).

This section will discuss the embedding process algorithm of the proposed system as (*Fig*. 2):

- Input: Logo and Cover images.
- Output: Watermark image.
- Process:

Step 1: Select the logo image and apply the preprocessing stage (convert the logo into gray level).

Step 2: Convert the logo image by using hologram transform (Fast Fourier transform) to generate the holographic logo image.

Step 3: Use three types of chaotic map (Logistic map, Arnold's cat map, or Baker map) to encrypt the Holographic logo image and calculate the measurement of each map.

Step 4: Select cover image.

Step 5: The Encrypted Holographic logo image is embedded into the cover image (step 3 with step 4) by using Least Significant Bit (LSB).

- End.

B. Extraction schema

In these steps the extraction process will discuss which is just the opposite of the embedding process.

- Input: Holographic Watermark image.
- Output: Logo and Cover images.
- Process:

Received 21/June/2021; Accepted 22/September/2021
© 2017 University of Technology, Iraq ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.1.5

Step 1: Take the Holographic Watermark image .
Step 2: Use XOR (inverse Least Significant Bit (LSB)).
Step 3: Obtained 2 images cover image and encrypted holographic logo image.
Step 4: Apply the inverse of the chaotic map (Logistic map, Arnold's cat map, or Baker map) to have the holographic logo imae.
Step 5: Convert the holographic logo image by using inverse of the hologram transform (Inverse Fast Fourier transform(IFFT)) to reconstract the original logo image.
- End.

VI. EXPERIMENTAL RESULTS

The experimental results are obtained by using 2 image, cover image and logo image, with two tests, test 1 contain Monkey image as a logo image and flowers image as a cover image, test 2 contain lenna image as a logo image and butterfly image as a cover image.

When logo image converted to holography form you can see more whiter region at the center showing low frequency content is more (*Fig. 3*. b, *Fig. 4*. b).

Peak to signal ratio (PSNR), Structural Similarity (SSIM), Mean square error (MSE), Root mean square (RMSE), and Normalize Root mean square (NRMSE) are used to compare between two images: the holographic logo image and the decrypted holographic logo image from chaotic map with the three types of chaotic maps, Entropy is calculated to the decrypted logo image as show in Table I and Table II.

Peak signal to noise ration abbreviation (PSNR), used to measure the ratio between the effective information of the image and the noise, can reflect whether the image is distorted. represents the difference between the maximum and minimum gray levels of the ideal reference image, which is usually 255 [22]. Mathematical representation equation below:

$$PSNR = 10 \log_{10} \left(\frac{MAX^2}{MSE}\right) \quad (4)$$

MAX^2 is the maximum possible pixel value of the image, MSE is the mean square error.
The larger the value of PSNR, the better the quality of the fused image and good transparency as shown in Table I, II the value of PSNR more than 32.

SSIM is an abbreviation of Structural SIMilarity, which indicates structural similarity. The value range is [-1,1]. In Table I, II obtained the SSIM value equal to 1, that mean the higher similarity and better the fusion quality. SSIM equation is:

$$SSIM(x,y) = \left(\frac{(2\mu_x\mu_y+c1)(2\sigma_{xy}+c2)}{(\mu_x^2+\mu_y^2+c1)(\sigma_x^2+\sigma_y^2+c2)}\right) \quad (5)$$

Where C1, C2, and C3 are constants, σ_x and σ_y = local sample standard deviations of x and y respectively, σ_{xy} = local sample correlation coefficient between x and y, μ_x and μ_y = local sample means of x and y respectively.
In Table I, II the value of the SSIM very close to 1, and that mean the holographic logo image and the decrypted holographic logo image both are very similar which means they have been maintained from deterioration.

Mean Square Error (MSE) reflects the degree of difference between variables and is an objective evaluation index of image quality based on pixel error. It is used to measure the difference between the

Received 21/June/2021; Accepted 22/September/2021
© 2017 University of Technology, Iraq ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.1.5

fused image and the ideal reference image. MSE is definitely non-negative, and should be as small as possible [23]. MSE given in formula bellow [24]:

$$MSE = \left(\frac{1}{mn}\right) \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} [I(i,j) - K(i,j)]^2 \quad (6)$$

Where m is the number of rows, n is the numbere of columns, i and j are the row and column pixels value of both the 2 images $I(i,j),\ K(i,j)$.
The lower value of the MSE mean lower error between the two images as shown in Table I, II that acheived about 34 – 37 value of the MSE.

Root Mean Square Error (RMSE) is computed by taking the square root of the squared error divided by the total number of pixels in the image [25].

$$RMSE = \sqrt{MSE} \quad (7)$$

NRMSE mathematical equation:

$$NRMSE = \left(\frac{\sqrt{MSE}}{\sum_{j=0}^{p} \frac{\max(d_j) - \min(d_j)}{p}} \right) \quad (8)$$

Where p=number of output processing elements, N= number of exemplars in the date set, d_j= desired output at processing element j.

Information entropy (H) (eq.9) is an objective evaluation index that measures the amount of information contained in an image and it is an important feature of uncertainty and randomness. The higher the information entropy, the greater amount of information in the fused image and for an ideally random image, the value of the information entropy should be close to 8.
The formula of information entropy is:

$$H = -\sum_{i-0,j=0}^{n-1} p_{(i,j)} \log_2 \left(p_{(i,j)}\right) \quad (9)$$

Where n = number of gray levels (256 for 8-bit images), p_k represents the probability of pixel gray level distribution i, j. The results of the computation of the information entropy of the encoded images are shown in Table I, II for test 1 and 2, The information entropy of the encoded hologram images is all very close to the value 6. Thus, the encoded hologram image has rather large randomsness, and leakage of image information is almost impossible. Therefore, the proposed algorithm can resist the entropy attack.

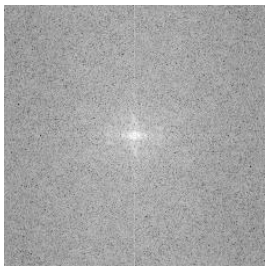
Histogram is calculated to the encrypted hologram image as show below in the *Fig. 3* and *Fig. 4* displays pixel value distribution in an image. In order to avoid statistical attacks Cipher images of a decent encryption scheme should have a uniformity histogram. The results clearly highlight the uniformity of the encrypted images as opposed to plain images (Watermarked image) as shown in (*Fig. 3*. h, j, l and *Fig. 4*. h, j, l).

Received 21/June/2021; Accepted 22/September/2021
© 2017 University of Technology, Iraq ISSN (Print) 1811-9212 ISSN (Online) 2617-3352

DOI: https://doi.org/10.33103/uot.ijccce.22.1.5

Test 1:

(a)

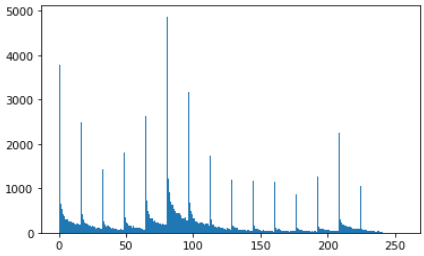


(b)

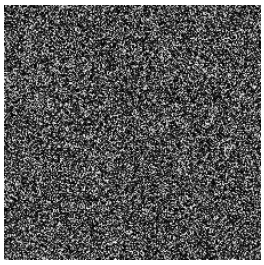
(c)

(d)

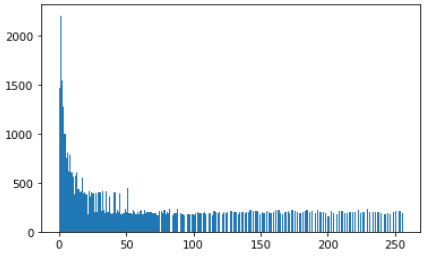
(e)



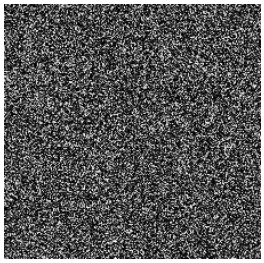
(f)



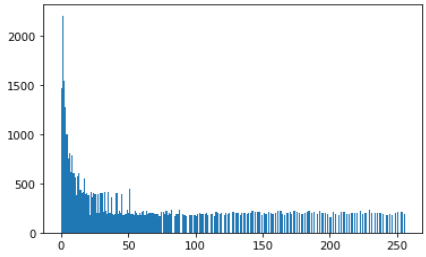
(g)



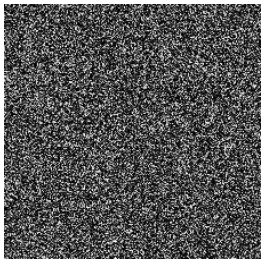
(h)



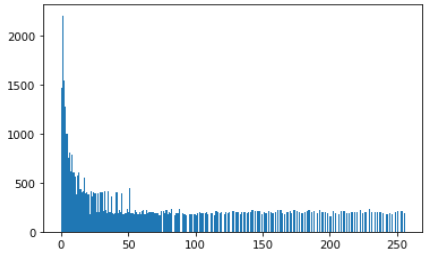
(i)



(j)



(k)



(l)

FIG. 3. (A) LOGO IMAGE. (B) HOLOGRAM LOGO IMAGE. (C) FLOWERS COVER IMAGE. (D) GRAY COVER IMAGE. (E)WATERMARK IMAGE (EMBEDDING). (F) HISTOGRAM OF (E). (G) ENCRYPTION OF (B) BY LOGISTIC MAP. (H) HISTOGRAM OF (G). (I) ENCRYPTION OF (B) BY ARNOLD MAP. (J) HISTOGRAM (I). (K) ENCRYPTION OF (B) BY BAKER MAP. (L) HISTOGRAM (K).

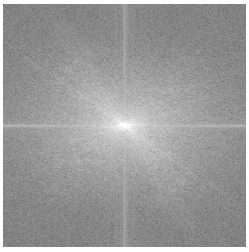
Received 21/June/2021; Accepted 22/September/2021

© 2017 University of Technology, Iraq *ISSN (Print) 1811-9212* *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.22.1.5

Test 2:

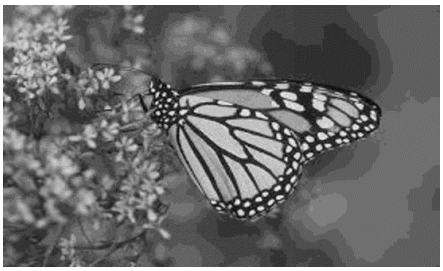
(a)



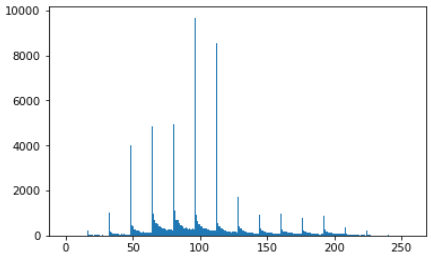
(b)

(c)

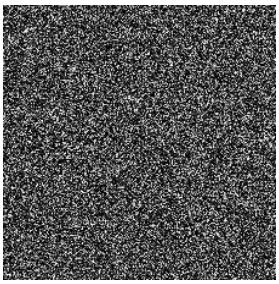
(d)



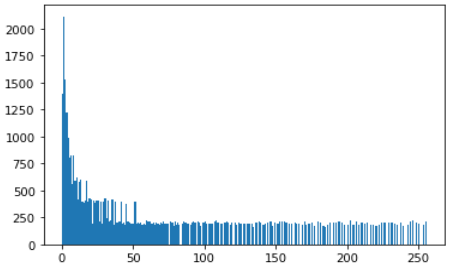
(e)



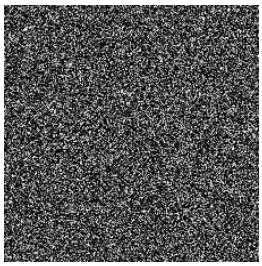
(f)



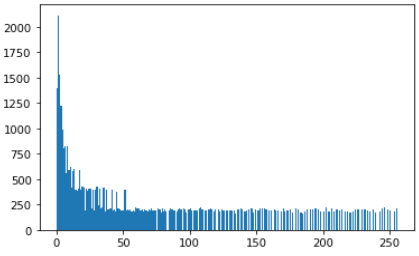
(g)



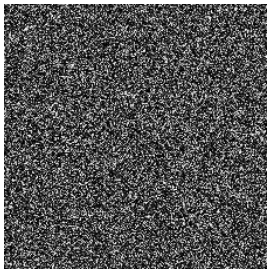
(h)



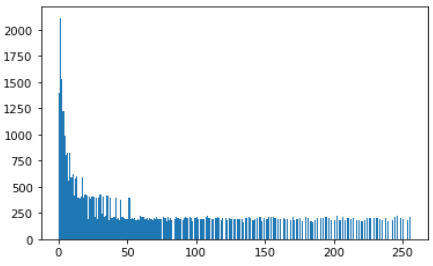
(i)



(j)



(k)



(l)

FIG. 4. (A) LENNA (LOGO IMAGE). (B) HOLOGRAM LOGO IMAGE. (C) BUTTERFLY IMAGE (COVER IMAGE). (D) GRAY COVER IMAGE. (E) WATERMARK IMAGE (EMBEDDING). (F) HISTOGRAM OF (E). (G) ENCRYPTION OF (B) BY LOGISTIC MAP. (H) HISTOGRAM OF (G). (I) ENCRYPTION OF (B) BY ARNOLD MAP. (J) HISTOGRAM (E). (K) ENCRYPTION OF (B) BY BAKER MAP. (L) HISTOGRAM OF (K).

Received 21/June/2021; Accepted 22/September/2021

© 2017 University of Technology, Iraq *ISSN (Print) 1811-9212* *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.22.1.5

TABLE I. MEASUREMENTS FOR TEST 1 (BETWEEN HOLOGRAPHIC LOGO IMAGE AND THE DECRYPTED HOLOGRAPHIC LOGO IMAGE)

Image	PSNR	SSIM	MSE	RMSE	NRMSE	Entropy
Logistic map	32.749	0.908	34.523	5.875	0.043	6.138
Arnold cat map	32.749	0.908	34.523	5.875	0.043	6.138
Baker map	32.749	0.908	34.523	5.875	0.043	6.138

TABLE II. MEASUREMENTS FOR TEST 2 (BETWEEN HOLOGRAPHIC LOGO IMAGE AND THE DECRYPTED HOLOGRAPHIC LOGO IMAGE)

Image	PSNR	SSIM	MSE	RMSE	NRMSE	Entropy
Logistic map	32.401	0.916	37.404	6.115	0.039	5.745
Arnold cat map	32.401	0.916	37.404	6.115	0.039	5.745
Baker map	32.401	0.916	37.404	6.115	0.039	5.745

VII. CONCLUSIONS

Digital image have become a regular part of our lives. Hence, it has increased in importance to provide processing and protection. A safe holographic watermarking technique based on chaotic encryption is suggested in this paper. The holograpic logo image encrypted by chaotic signals can be generated by structurally complex dynamic systems and over a long time cannot be predicted, and it can replicate the chaotic sequence only according to initial parameters. The reason of transformed the logo image to into a hologram is to increase the security of watermark information, Safety of the transmission of your information, and to recover the robustness of the watermark algorithm. Therefore, the security of the watermark algorithm has improved.

REFERENCES

[1] H. B. Abdulwahab and S. F. Amir, "Efficient Digital Watermark key Generation Using Hexagonal Structure and parametric Lagrange Curve," *Eng. &Tech.Journal*, vol. 33, no. 2, pp. 192–203, 2015.

[2] M. Saiful Islam, M. A. Ullah, and J. P. Dhar, "An imperceptible & robust digital image watermarking scheme based on DWT, entropy and neural network," *Karbala International Journal of Modern Science*, vol. 5, no. 1, 2019.

[3] B. S. Mahdi and A. Karim, "Hybrid Techniques for Proposed Intelligent Digital Image Watermarking," *Eng. & Tech. Journal*, vol. 33, no. 4, pp. 702–713, 2015.

[4] T. Venugopal and V. S. K. Reddy, "Image watermarking using two level encryption method based on chaotic logistic mapping and Rivest Shamir Adleman algorithm," *International Journal of Intelligent Engineering and Systems*, vol. 11, no. 6, pp. 271–281, 2018.

[5] J P Pang, A L Wang, X F Zhu, L Guo, S K Li, K Xin, S X Fan and F P Liu, "A holographic image robust watermarking algorithm based on DWT-SIFT and neural network model," *IOP Conf. Series: Materials Science and Engineering*, 2019.

[6] H. M. Yousif Al-Bayatti, A. M. S. Rahma, and H. B. Abdulwahab, "Using generated digital images to modify the PGP cryptography protocol," *Proceedings of The 2007 International Conference on Security and Management, SAM'07*, no. January 2017, pp. 147–151, 2007.

[7] N. Kumar, D. Wadhwa, D. Tomer, and S. Vijayalakshmi, "Review on Different Chaotic Based Image Encryption Techniques," *International Journal of Information and Computation Technology*, vol. 4, no. 2, pp. 197–206, 2014.

[8] R. Jin and J. Kim, "Rotation-Invariant Image Watermarking Scheme Based on Radon Transform," no. March 2017, pp. 753–758, 2015.

Received 21/June/2021; Accepted 22/September/2021

© 2017 University of Technology, Iraq *ISSN (Print) 1811-9212* *ISSN (Online) 2617-3352*

DOI: https://doi.org/10.33103/uot.ijccce.22.1.5

[9] L. Wang, F. Liu, Z. Fu, Y. Wang, and Z. Lu, "Digital Watermarking Technology of Holographic Image Based on S-FFT Method," *2nd International Conference on Artificial Intelligence and Industrial Engineering (AIIE2016)*, vol. 133, no. 2, pp. 240–243, 2016, doi: 10.2991/aiie-16.2016.56.

[10] X. Zhou, H. Zhang, and C. Wang, "A robust image watermarking technique based on DWT, APDCBT, and SVD," Symmetry (Basel), vol. 10, no. 3, 2018.

[11] S K Li, A L Wang, J P Pang, L Guo, K Xin, S X Fan, and F P Liu, "Research on Robust Algorithm of Color Holographic Watermark Based on DCT-DWT," *IOP Conf. Series: Materials Science and Engineering*, 2019.[1]

[12] Z. Liu, A. Wang, K. Xin, F. Liu, and X. Zhu., "Digital Holographic Watermarking Algorithm Based on DWT-DCT," *Journal of Physics: Conference Series*, vol. 1693, no. 1, pp. 68–74, 2020.

[13] Cox I., Miller M., Bloom J., Fridrich J., and Kalker T., "Digital watermarking and steganography," Morgan Kaufmann, Second Edition, 2007.

[14] Rathi S. C. and Inamdar V. S., "Medical images authentication through watermarking preserving ROI," *Health Informatics-An International Journal (HIIJ)*, Volume 01, Issue 01, 2012.

[15] K. M. Hosny, "Multimedia Security Using Chaotic Maps: Principles and Methodologies," Vol. 884. New York: Springer, 2020.

[16] J. G. Sekar and C. Arun, "Comparative performance analysis of chaos based image encryption techniques," *Journal of Critical Reviews*, vol. 7, no. 9, pp. 1138–1143, 2020.

[17] K. Gopakumar, and Rija M. Raju, "A novel watermarking technique based on chaos theory," *International Journal of Applied Engineering Research*, ISSN 0973-4562 Volume 8, pp. 1081-1089, 2013.

[18] A. Waghmare, A. Bhagat, A. Surve, and S. Kalgutkar, "Chaos Based Image Encryption and Decryption," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 4, pp. 64–68, 2016.

[19] A. A. Alabass, M. A. Hayder, Z. Salah, O. L. A. H. Rasool, and M. A. Hasan, "Color Image Encryption and Decryption by Using Chaotic Baker Map Bit Interleaver," *International Research Journal of Engineering and Technology (IRJET)*, vol. 4, no. 5, pp. 382–385, 2017.

[20] D. Asamoah, E. Ofori, S. Opoku, and J. Danso, "Measuring the Performance of Image Contrast Enhancement Technique," *Int J Comput Appl*, vol. 181, no. 22, pp. 6–13, 2018.

[21] A. D. Salman and H. B. A. Wahab, "Study Analysis to New Trend for 3D Video Watermark", *Revista Aus*, vol. 26–2, 2019.

[22] A. A. Kareem, A. M. S. Rahma, and H. H. salih, "A Statistical Image Noise Removal Adaptive Filter Using Rejection Test with F- Distribution," *Eng. &Tech.Journal*, vol. 32, no. 2, pp. 302–312, 2014.

[23] H. B. Abdulwahab, K. L. Hameed, and N. H. Barnouti, "Video authentication using PLEXUS method," *International Journal of Advanced Computer Science and Applications*, vol. 9, no. 11, pp. 730–737, 2018.

[24] M. R. Muqri, E. J. Wilson, and J. Shakib, "A taste of python - Discrete and fast fourier transforms," *ASEE Annual Conference and Exposition, Conference Proceedings*, vol. 122nd ASEE, no. 122nd ASEE Annual Conference and Exposition: Making Value for Society, 2015.

[25] M. S. Kovalev, S. B. Odinokov, P. A. Ruchka, and N. G. Stsepuro, "The usability of discrete representation of holograms," *Journal of Physics: Conference Series*, vol. 1096, no. 1, 2018.

Received 21/June/2021; Accepted 22/September/2021

© 2017 University of Technology, Iraq *ISSN (Print) 1811-9212* *ISSN (Online) 2617-3352*