Journal of Kerbala University , Vol. 14 No.1 Scientific . 2016

Authentication and Secure Image System Based on Combining Image Cryptography and Digital Watermarking

نظام توثيق وتأمين الصورة بناء على الجمع بين تشفير الصور و العلامة المائية الرقمية

Abstract Manaf Mohammed Ali
Karbala University
Manafma77@gmail.com

Abstract:-

Due to The increase of using the international network, the multimedia data security becomes the most significant factor to protect data. Encryption algorithms are covers some of data security requirement like confidentiality, prevent eavesdropping of data and integrity but the others requirements like copyright protection and data authentication which can be satisfy by sharing with another security technique which is called digital watermarking. So in this paper, digital watermarking and image encryption algorithm based on chaotic map are merging in one system to satisfy these objectives. The experimental results show The proposed scheme has a high security and, the correlation coefficients approach to zero(0.008) and high speed(0.5)second with good quality of extracted image after decrypted image(37dB).

Key words: Digital Watermarking, Cryptography, Spatial domain, Authentication

المستخلص

نتيجة للزيادة في استخدام الإنترنت ، أمنية بيانات الوسائط المتعددة أصبحت أهم عامل لحماية البيانات. خوارزميات التشفير توفر بعض متطلبات أمن البيانات مثل السرية و منع التنصت على البيانات و سلامتها ولكنها لا توفر متطلبات أخرى مثل حماية حق المؤلف و توثيق البيانات والتي يمكن تحقيقها من خلال المشاركة مع تقنية أمنية أخرى وهو ما يسمى بالعلامة المائية الرقمية . لذا في هذه البحث ، العلامة المائية الرقمية وخوارزمية تشفير الصورة على أساس معادلة الفوضى قد دمجت في منظومة واحدة لتحقيق هذه الأهداف. أظهرت النتائج التجريبية بأن النظام المقترح لديه أمنية متينة, معاملات الارتباط تقترب للصفر(0.008) و سرعة عالية (0.5) ثانية مع جودة جيدة للصورة المستخرجة بعد فك التشفير(37dB) .

1. Introduction

The use of public networks or internet growing rapidly every day and the need to display and transmission multimedia data on these networks become necessary .Multimedia data diffuse in different sides of the internet applications like YouTube, Facebook, Electronic Mail and some of these should be private like military data, medical data and video conferencing etc.

So today's world it is very much essential to secure the data being transmitted over a communication channel and this can be accomplished by cryptography or watermarking [1].

The basic terminology is that cryptography refers to the science and art of designing ciphers; cryptanalysis to the science and art of breaking them; while cryptology, often shortened to just crypto, is the study of both. The input to an encryption process is commonly called the plaintext, and the output the ciphertext [2].

Digital watermark is a symbol of ownership in natural and non-natural(document)images to verify the identity of its owners and data authentication. The digital data might be images, audios or videos and the embedded information could be an image or textual data to verify the owner such as the name of the author, signature[3].

The main process of the watermarking is similarly as the handwritten signature. It's like paper signature and it having the digital certificate using this verifies the identity.

According to working domain ,the watermarking techniques can be divided into types

a) Spatial domain watermarking techniques.
b) Frequency domain watermarking techniques.

In spatial domain techniques, the watermark embedding is done on image pixels while in frequency domain watermarking techniques the embedding is done after taking image transforms[4]

Also watermarking techniques can be divided into four types according to the type of document to:

- Image watermarking
- Video watermarking
- Audio watermarking
- Text watermarking

Encryption gives techniques for securing the integrity and authenticity of transfer of information. Encrypted data cannot be interpreted and need to be decrypted at the receiving end. Therefore, in addition to encryption, a Watermarking technique is used for embedding logo or label data to digital information being transmitted. These two techniques are complementary rather than overlapping and can be combined to increase protection of the message [5].

2. Chaotic Theory

Chaotic theory has been established in 1970s from many different research areas, such as physics, mathematics, biology and chemistry. Chaos is an inherent property of a class of nonlinear and dynamic systems[6]. Chaotic systems have different characteristics. The most important are:

- **Deterministic:** This means that they have some determining mathematical equations ruling their behavior.
- **Ergodicity**: Statistical measurements of the variables give similar results no matter if they are performed over time or space. Put it in another way, the dynamics shows similar statistics when measured over time or space.
- **Aperiodicity**: The system evolves in an orbit that never repeats on itself, that is, these orbits are never periodic
- **Unpredictable and non-linear**: This means they are sensitive to initial conditions. even a very slight change in the starting point can lead to a significant different outcome.
- **Appear to be random** and disorderly but in actual fact they are not. Beneath the random behavior, there is a sense of order and pattern[7].

3. The Relationship Between Cryptography and Chaotic Theory

Each cryptography systems depends on two concepts which are confusion and diffusion, Confusion refers to making the relationship between the key and the ciphertext as complex and involved as possible. Diffusion refers to the property that redundancy in the statistics of the plaintext is ”dissipated” in the statistics of the ciphertext [8]. Diffusion is associated with the dependency of the output bits on the input bits. In a cipher with good diffusion, changing one bit should change each output bit with a probability of one half. Due to these concepts there are good relationship between chaotic theory and cryptography as shown in Table[1]

Table (1) The connection Between Chaos and Cryptography.

Chaotic Characteristic	Cryptographic property	Description
Ergodicity Mixing property Auto-similarity	Confusion	The output of the system seems similar for any input.
Sensitivity to initial conditions and control parameters	Diffusion	A small difference in the input produces a very different output
Deterministic	Deterministic Pseudo randomness	A deterministic procedure that produces pseudo randomness
Complexity	Algorithmic complexity	A simple algorithm that produces highly complex outputs

4. Applications of Digital Watermarking

Multimedia represents the backbone of public networks like internet, So digital watermarking can be used in different trends specially in multimedia field, some applications of watermarks are listed below[9].

Copy protection: Digital content can be watermarked to indicate that the digital content cannot be illegally replicated. Devices capable of replication can then detect such watermarks and prevent unauthorized replication of the content [10].

Copyright protection: Digital watermarking can be used to identify and protect copyright ownership. Digital content can be embedded with watermarks depicting metadata identifying the copyright owners.

Fingerprinting: In order to trace the source of illegal copies, the owner can embed different watermarking keys in the copies that are supplied to different customers. For the owner, embedding a unique serial number-like watermark is a good way to detect customers who break their license agreement by copying the protected data and supplying it to a third party.

Broadcast monitoring: Over the last few years, the number of television and radio channels delivering content has notably expanded. And the amount of content flowing through these media vehicles continues to grow exponentially. In this highly fragmented and fast changing market, knowing the real broadcast reality has become critical for content owners, copyright holders, distributors and broadcasters

Content Archiving: Watermarking can be used to insert digital object identifier or serial number to help archive digital contents like images, audio or video. It can also be used for classifying and organizing digital contents. Normally digital contents are identified by their file names; however, this is a technique as file names can be easily changed. Hence embedding the object identifier within the object itself reduces the possibility of tampering and hence can be effectively used in archiving systems [11].

Meta-data Insertion: Meta-data refers to the data that describes data. Images can be labeled with its content and can be used in search engines. Audio files can carry the lyrics or the name of the singer. Journalists could use photographs of an incident to insert the cover story of the respective news. Medical X-rays could store patient records[11].

5. Related Works

Few approaches have been suggested to merge cryptography with watermarking without overlapping in job as listed below.

Hama S. Meharwade and…etal.[12]. proposed a joint encryption and watermarking technique for images. The encryption algorithm is based on Arnold cat map and S-box substitution and the watermarking technique is carried out in the DCT domain. The results show, the correlation coefficients is low, immunity against differential attack.

Preeti Gupta [13] proposed a blind watermarking technique that uses watermark nesting and encryption. Nesting means it embeds an extra watermark into the main watermark and then embeds the main watermark into the cover image. For embedding watermarked watermark in Cover Image used DWT based technique. It can embed more number of watermark bits in the gray scale cover image without affecting the imperceptibility and increase the security of watermarks.

Mr.Sudhanshu and Ashok A.Ghatol [14] are proposed Combination of encryption and digital watermarking techniques used for security and copyright protection of still image. It used advanced encryption standard technique for the security of digital watermark and frequency domain technique is used in digital watermarking technique for copyright protection with the help of discrete cosine transform.

W. Puech and M. Rodrigues[15] are proposed a method that combines image encryption and watermarking technique for safe transmission purpose. This method is based on the combination of public-private keys and secret key ciphering, and watermarking.

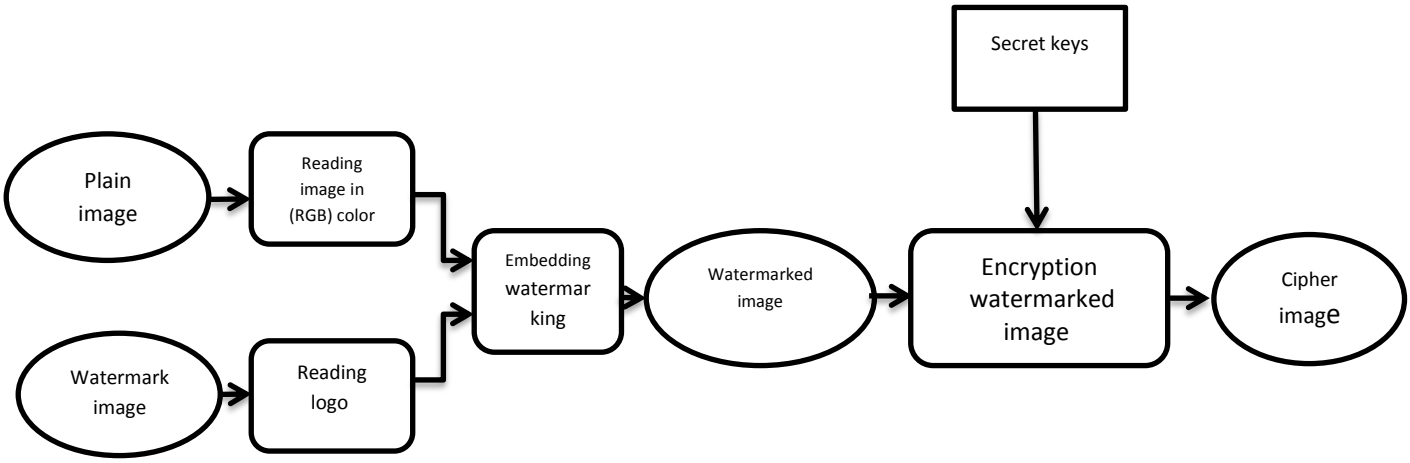
Each one of above schemes are determine corresponding to the area of application. In this paper, proposed the combined scheme, the encryption operation depend on chaotic theory to satisfy the high protection, decrease the execution time and visible watermarking in spatial domain to copy right protection and avoid unauthorized replication of the image. These operations are processed without overlapping and complement each other.

6. The Proposed Scheme

The cryptography aims to protect data and satisfy confidentially and prevent eavesdropping of data but the Watermarking is the process to embedding data called a watermark for digital signature or logo into a multimedia object to purpose of copyright protection and data authentication, So in this paper digital image watermarking and cryptography are merging to satisfying secrecy, integrity, copyright protection and identity of media ownership.

Two techniques have been processed to implement this project. The first one was implement watermark technique by embedding the logo or label in the original or host image and the result was image watermarked and then apply. The second step was encrypted image watermarked based on 2D nonlinear equations and the result was encrypted image.

These operations which occurred in embedding process and encryption process are shown in encryption and watermarking model Figure (1).



Figure(1): Model for Image Encryption and Watermarking

There are set of steps to embedding a watermark and encryption image as the following in these stages:

1. Read host or original image (256*256)pixels.
2. Read watermark image or logo(32*32)pixels.
3. Embedding watermark image into top left of original image, the result of this operation is watermarked image by using visible watermarking based on this equation:

$$F_w = (1-a)F + a * W \qquad \ldots\ldots(1)$$

Where, F_w= watermarked image ,
a=constant , $0 \le a \le 1$
If a= 0 then no watermark, If a=1 the watermark present F=original image, W= watermark image [16]

4. Encryption the watermarked image based on non- linear equation (2D chaotic standard map), two operations are processed in this step

a) Permutation: To shuffle position of image pixels
b) Substitution or Diffusion : To change the values of image pixels.

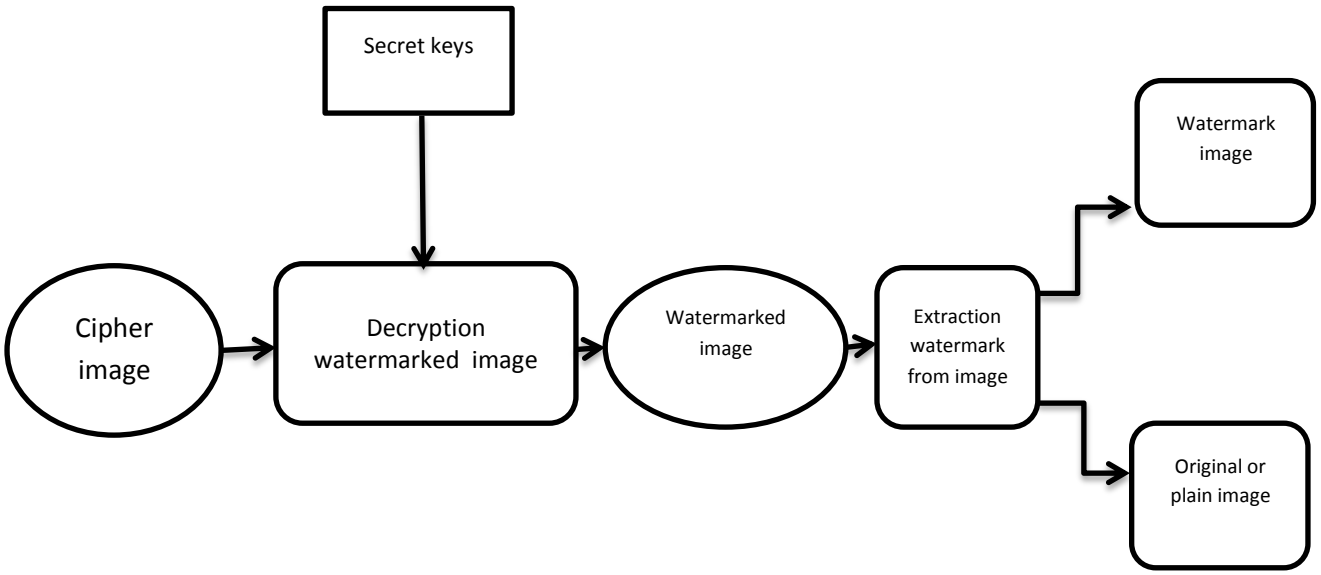
$$x_{k+1} = (x_k + y_k + r_x + r_y) \bmod (n)$$

$$y_{k+1} = \left[y_k + r_y + k_c \sin\left(\frac{2\Pi \; x_{k+1}}{n} \right) \right] \bmod (n) \qquad \ldots.(2)$$

Where (x_k , y_k) and (x_{k+1} , y_{k+1}) is the original and the permuted pixel position of an N × N image respectively. Where n is the image width and height, (r_x , r_y) is a random scan couple, and standard map parameter K_c is a positive integer[17].

5. The output of this procedure is a cipher watermarked image.

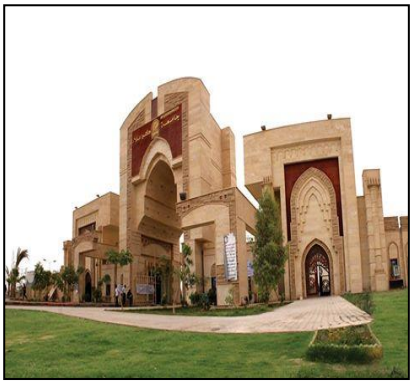
In the side of decryption and extraction of watermarked image ,the above operations will be occurred but in the inverse direction as shown in Figure (2)



Figure(2): Model for Image Decryption and Extraction Watermark

7. Evaluation And Experimental Results

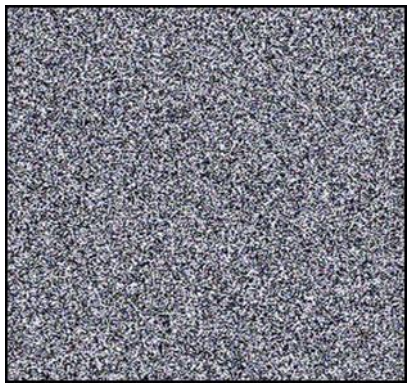
To evaluate any scheme, there are different criteria and different cases to test any system. When we are merge watermarking with image cryptography system and the results as shown in Figure (3) then the criteria must be related to these fields. So these criteria are(processing time, Key space, correlation coefficient and the watermarking quality, capacity of watermark). Many images are tested like(cameraman, Freedom square, Karbala university, Airplane, Lena) and different logos and labels as watermark. The scheme was implemented under programing language (VB 2008).



(1) Karbala Uni. Image

(2)Watermark Logo Image

(3) Watermarked image



(4) Cipher image

(5)Decryption of watermarked image

Figure (3): plain image (Karbala Uni. image) (1), Logo image(2), watermarked image(3), cipher image(4), Decrypted image(5).

A. Processing Time

The system included two operations, watermark operation and encryption operation therefore there is delay time when process each one. The execution time of these operations are shown in Table (2), Whenever the number of iterations in the encryption operation= 10 Rounds.

Table(2): The processing time of embedding and encryption operations

Images	Processing Time(SEC)		
	Embedding Watermark Time	Encryption Time	The Total Time
Karbala uni.	0.25	0.28	0.57
Lena	0.25	0.31	0.56
Airplane	0.12	0.26	0.38
Cameraman	0.11	0.27	0.38

The speed of data security scheme represents the most significant criterion specially when the security is related to multimedia security at online application which need to increase the speed of scheme based on fast algorithms. From the above table , we observe the total execution time for these operations is less than (1 second) therefor the scheme is suit for different applications like real time application.

B. Correlation Coefficient

A correlation determines the relationship between two variables. In other words, correlation is a measure that computes degree of similarity between two variables. Correlation coefficient is a useful measure to judge encryption quality of any cryptosystem[18]. Correlation coefficient is useful to evaluate and judge the quality for any scheme, the scheme appear to random and hide the properties of image when the correlation between the adjacent pixels is approach to zero .

If encrypted image and plaintext image are completely different then their corresponding correlation coefficient must be very low, or very close to zero. The correlation coefficient of the pixel pair is then calculated as in equation (3)

$$r_{xy} = \frac{\mathrm{cov}(x, y)}{\sqrt{D(x)D(y)}}, \qquad \text{.....(3)}$$

Where ***x*** and ***y*** represent gray-scale values of two pixels in the same place in the plaintext and cipher text images. *D(x)* is variance at pixel value x in the plaintext image and *Cov(x,y)* is covariance at pixels x and y for both the plain-image and the cipher image.

Tables (3) represents the correlation coefficient for watermarked image and cipher watermarked image. Figure (4) shows the difference between correlation values before and after processing.

Table (3) Correlation coefficient for watermarked image and cipher watermarked image

Images	Vertical		Horizontal		Diagonal	
	Plain image	Cipher image	Plain image	Cipher image	Plain image	Cipher image
Karbala Uni.	0.983	0.00923	0.9367	0.00832	0.9563	0.0075
Lena	0.9643	0.00955	0.9506	0.01711	0.9353	0.0231
Airplane	0.9221	0.00759	0.9353	0.01275	0.8832	0.0234
Cameraman	0.9728	0.00581	0.9498	0.00864	0.8925	0.0114

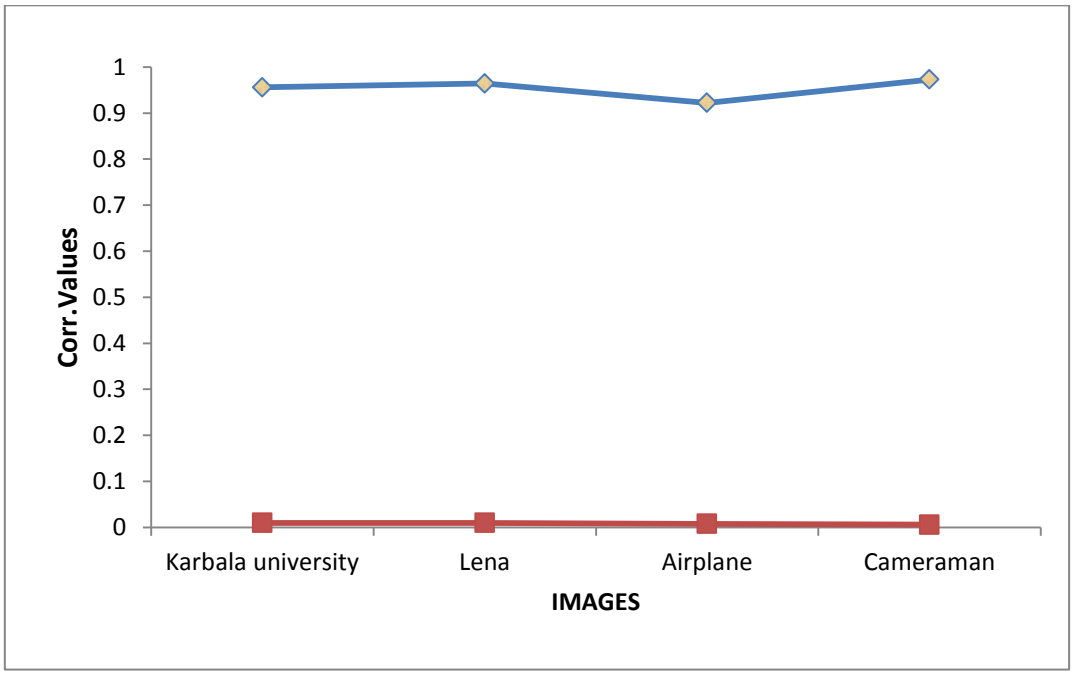


Figure (4): The difference values between correlation coefficients (Vertical)

The correlation criteria are apply to evaluate the similarity between adjacent pixels of image. whenever the similarity is less, then the correlation is approach to zero and the results is appear randomly. From Table(3) and Figure (4), we can see that results are closer to zero, the output image is a distorted image. So the algorithm which used to encrypt the image has non-linear features and immunity to different attacks like statistical attack.

C. Key Space Analysis

1. Exhaustive Key Search Test

Theoretically, the large key space lead to strength cipher and it's difficult to break by attackers specially brute force attacks, so one of the significant matter in encryption schemes is enlarge key space . In this paper, two levels of encryption are applied which perform two processes permutation and diffusion, The key space (when we use same keys for different iterations (n))). Then the key space = [(N2)!]. So the key space is very large and difficult to crack this algorithm when the final key space is equal to (permutation +diffusion) key space .

2. Key Sensitivity Test

One of the best factors to test the encryption algorithm is the sensitivity of The key parameters so the encryption algorithm is good and difficult to break by attackers when its sensitive to any change in the key parameters until if it a slight change. The attacker try to change the key parameters continually to get and reach the relationship between the plain and cipher image and reveal the secret key.to evaluate the sensitivity of this project, the same key parameters are used in the encryption and decryption side unless one slight change in positive parameter key (K_c=850)in encryption side and (K_c=851)in decryption side as shown in figure(5).

(A) (B)

(C) (D)

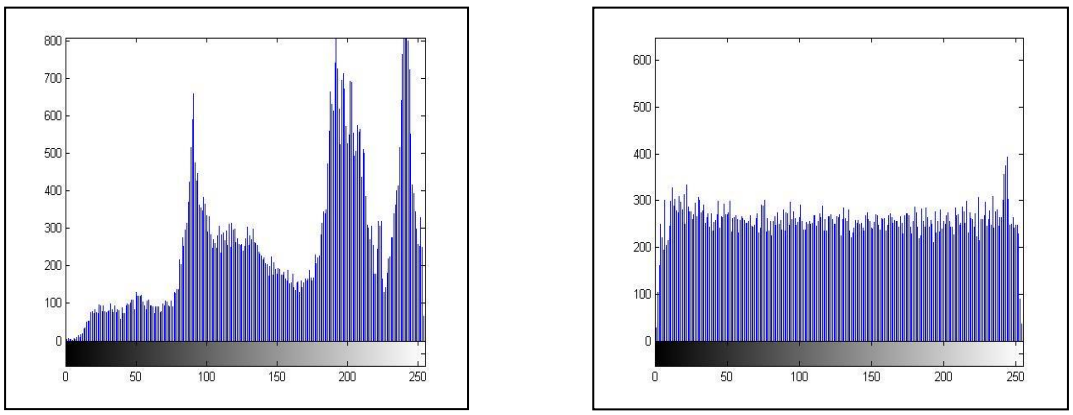
Figure(5): (a) Plain watermarked image " Freedom square.bmp "; (b) cipher image; (c) decryption image with only one bit is differ in standard map parameter k_c = 851 and (d) decryption watermarked image with same parameter(k_c=850).

Clearly, From the above Figure the scheme is sensitive to any change in the secret keys which is refer to the critical features of scheme, also the practical results show its sensitive to any slight change in the watermark image or the number of iterations.

D. Histogram or Statistic Characteristic of Images

Image histogram is appear the statistical characteristics of image, color histogram is a representation of the distribution of colors in an image which can directly reflect the correlation of the gray value and the frequency of the gray value in the image[19].

As shown in figures (6), the plain image **(The freedom square.bmp**) and its relative corresponding cipher image are presented, their histograms are presented too.



(A) **(B)**

Figure(6): (A) Histogram of Freedom square image (B) Histogram of cipher image for Freedom square image

Clearly, the histograms are difference between Figure (6-A)and Figure(6-B). The distribution of pixel values in figure(6-A)is more uniform than Figure(6-B), therefore it hides the statistical attributes of the original image .As a result, it prevents the attackers to trace or estimate the original image.

E. Imperceptibility

To test the quality of watermarking techniques, Imperceptibility means that the perceived quality of the host image should not be distorted by the presence of the watermark. To measure the quality of a watermarked image, the peak signal to noise ratio (PSNR) is used. The PSNR (in dB) is defined as:

$$PSNR = 20\log_{10}\left(\frac{MAX_f}{\sqrt{MSE}}\right) \qquad \text{.....(4)}$$

The equation computes the maximum possible value using 8 bits plane.

$MAX_f=2^8-1=255$

$$MSE = \frac{1}{mn}\sum_{0}^{m-1}\sum_{0}^{n-1}\|f(i,j)-g(i,j)\|^2 \qquad \text{.....(5)}$$

Where: m*n=size of original host image and watermarked image
F(i,j) =pixel value of original host image
g(i,j) = pixel value of watermarked image

larger PSNR value indicate high watermarked image quality, when the value under (30 dB) indicate low quality (the noise added when the processed embedding and encryption)and the difference between the original image and extracted image is high.

Table (4) shows the results of calculating PSNR for some images.

Images	Karbala Uni.	Cameraman	Lena	Airplane
PSNR(dB)	37	37.4	36.5	36.5

From above table, the value of PSNR is greater than (30 dB), so the image extraction after watermark and encryption is acceptable.

F. Capacity of watermark

It refers to the rate of data which can be embedded into original image. The suggestion scheme is adopted image watermarking in the spatial domain, so the average data that embedded is depend on the size of the image, generally is high capacity in comparison with frequency domain .

8. Conclusions

Due to the widespread of internet that require the huge amount of multimedia content specially images. data security become very necessary to save the privacy of these data, Sometimes The visual encryption may be not enough to protect these images.it not provides security after the content is decrypted Therefore joint digital watermarking with images encryption to satisfy the integration and achieve the security requirements, where digital watermarking is used to verify the authenticity or identity of its owner by embedding watermark in to the host image which used for copy right protection while the cryptography is used to verify the identity of the data receiver by using secret keys. The experimental result show the system has high watermarking capacity , good imperceptibility (PSNR=37 dB), fast in processing time (0.5)second for two operations , high security because it has large key space, uniform histogram and the correlation coefficient approach to zero (0.00832).

References

[1] Hama S Meharwade ,Veena S, Arthi R Shankar " ***Joint encryption/watermarking based on Arnold cat map and DCT***" International Journal of Software & Hardware Research in Engineering,Volume 3 Issue ,india, 2015.

[2] IngemarJ.Cox, Gwenael. Doerr, Teddy Furon" ***Watermarking Is Not Cryptography***" University College London, France, 2006.

[3] Saba,T. and Altameem,A."***Analysis of Vision based Systems to Detect Real Time Goal Events in Soccer Videos***" Applied Artificial Intelligence,27,656-67,2013.

[4] Pooja Dabas and Kavita Khanna " ***A Study on Spatial and Transform Domain Watermarking Techniques***" International Journal of Computer Applications (0975 – 8887) Volume 71– No.14, May 2013

[5] Robert, L., and T. Shanmugapriya, "***A Study on Digital Watermarking Techniques*** ", International Journal of Recent Trends in Engineering, Volume . 1, No. 2, pp. 223-225, 2009.

[6] Mazleena Salleh; Subariah Ibrahim; Ismail Fauzi Isnin; " ***Enhanced chaotic image encryption algorithm based on Baker's map***, " Circuits and Systems, 2003. ISCAS '03. Proceedings of the 2003 International Symposium on , Pages:11-508 - 11-511 Volume: 2 , 25-28 May 2003.

[7] Ahmad Alkhatib and Marwan Krunz; "***Application of Chaos Theory to the Modeling of Compressed Video,***" Communications, 2000. ICC 2000. 2000 IEEE International Conference on , Volume: 2, Pages:836 - 840 vol.2, 18-22 June 2000.

[8] Volodymyr Lynnyk "***Chaos-based Communication Systems***," Doctoral thesis, Czech Technical University in Prague, Faculty of Electrical Engineering, Prague, 2010.

[9] Ensaf Hussein, Mohamed A. Belal, ,"***Digital Watermarking Techniques, Applications and Attacks Applied to Digital Media***", IJERT, ISSN: 2278-0118, Vol. 1 Issue 7, September-2012.

[10] Jiang Xuehua "***Digital Watermarking & its Application in image copyright Protection***" published in proceedings of International Conference on Intelligent Computation Technology & Automation ICICTA, 2010.

[11] Vinita Gupta Mr. Atul Barve **" *A Review on Image Watermarking and its technique"*** I JMEIT Vol. 2, Page No: 73-81, Issue 1, Jan 2014**.**

[12] Hama S Meharwade ,Veena S, Arthi R Shankar " ***Joint encryption/watermarking based on Arnold cat map and DCT"*** International Journal of Software & Hardware Research in Engineering, Vol. 3, India, 2015.

[13] Preeti Gupta **" *Cryptography based digital image watermarking algorithm to increase security of watermark data"*** International Journal of Scientific & Engineering Research, Vol. 3, Issue 9, September 2012**.**

[14] Mr.Sudhanshu Suhas, Mr.Ashok A.Ghatol" ***Combination of Encryption and Digital Watermarking Techniques used for Security and Copyright Protection of Still Image"*** IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), May 09-11, India. 2014.

[15] W Puech and 1.M. Rodrigues." ***A new Crypto-Watermarking Method For Medical Images Safe Transfer***" university of montpellier ii 161, rue ada, 34392 Montpellier codex 05, France.2005.

[16] Kamal Kant, Ruchi Doshi ***"Robust &secure digital image watermarking technique using concatenation process"*** International journal of ICT and management, Vol. 1, ISSN NO.2026-6839, 2013.

[17] S.G. Lian, J. Sun, Z. Wang**, "*A block cipher based on a suitable use of the chaotic standard map*",** Chaos, Solitons & Fractals 26 (1) pp. 117-129, 2005.

[18] Hemlata Agrawal, Narendra Kahtr "***Image Encryption using Various Transforms-A Brief Comparative Analysis***" IEEE, International Conference on Magnetics, Machines & Drives, India, 2014.

[19] Mr.J.Nagaraj Jaya Sridhar, Mr. K.Moorthi "***Reversible Watermarking Based on Encryption Image Classification and Dynamic Color Techniques***" International Conference on Engineering Technology and Science Vol. 3, Special Issue 1, February 2014

.