DOI:10.24996/ijs.2018.59.1C.19

Iraqi Journal of Science

ISSN: 0067-2904

E-commerce Application Based on Visual Cryptography and Chen's Hyperchaotic

Hala Bahjat Abdul Wahab,Thikra M. Abed*

Department of Computer Science, University of Technology, Baghdad, Iraq

Abstract

This paper proposed to build an authentication system between business partners on e-commerce application to prevent the frauds operations based on visual cryptography shares encapsulated by chen's hyperchaotic key sequence. The proposed system consist of three phases, the first phase based on the color visual cryptography without complex computations, the second phase included generate sequence of DNA rules numbers and finally encapsulation phase is implemented based on use the unique initial value that generate in second phase as initial condition with Piecewise Linear Chaotic Maps to generate sequences of DNA rules numbers. The experimental results demonstrate the proposed able to overcome on cheating attacks, exhaustive attack, and resistant the statistical attack.

Keywords: E-commerce, Visual Cryptography, Chen's hyper-chaotic, DNA computing, Runge-Kutta method.

تطبيقات التجارة الالكترونية بالاستناد على التشفير المرئي والفوضى الهجينة

هالة بهجت عبدالوهاب، ذكرى محمد عبد*

قسم علوم الحاسوب، الجامعة التكنلوجية، بغداد، العراق.

الخلاصة

اقترحت هذه الورقة لبناء نظام للتأكد من موثوقية اطراف الاعمال في تطبيقات التجارة الإلكترونية لمنع عمليات الاحتيال وذلك بالاعتماد على اسهم التشفير البصري المغلفة بسلسلة مفتاح من فرط الفوضى. النظام المقترح يتكون من ثلاث مراحل، المرحلة الاولى تعتمد على التشفير المرئي الملون الذي لا يحتاج الى حسابات معقدة ، المرحلة الثانية تتضمن توليد سلسلة من ارقام قوانين واخيرآ مرحلة التغليف يتم تنفيذها بالاعتماد على استخدام قيمة اولية غير مكررة والتي ولدت في المرحلة الثانية كشرط أولي مع لتوليد سلسلة من ارقام قوانين . النتائج التجريبية اوضحت بان المقترح قادر على التغلب على هجمات الغش، الهجوم الشامل، ومقاومة الهجوم الإحصائي.

1. Introduction

Electronic-commerce (E-commerce) define as using data and communication technology to online shopping and marketing of the products and involves the transfer of cash. Peoples have a tendency to live in digital world, wherever the Personal Computers (PCs) and computer networks helps to perform the most of the business dealings. The PC and networks offer platform to do e-commerce tasks, on-line banking, and sharing of data between the business parties in a fraction of seconds in any places of the digital world. Two functions are needed to safety the e-commerce applications, they are:
i) guard customers' privacy.
ii) guard against fraud.

Whereas quite 2 parties communicate to every alternative then they worry regarding confidentiality, knowledge authentication, nonrepudiation etc.[1]. To execute the increasing demand of security, many security techniques providing this scenario and Visual cryptography is one of them [2].

*Email: thikra_mohamed@yahoo.com

Visual cryptography (VC) is a special type of sharing secrets. It encodes the target visual into several carrier images which are printed on transparencies. VC can be applied to different areas copyright protection, secret message sharing, and watermarking [3].

DES, IDEA and RSA are the classical algorithms and not suitable for practical image encryption. The super-speed and low costs makes the chaotic cryptosystem better candidates than many other encryption algorithms for image encryption [4].

Deoxyribonucleic acid sequence (DNA) technology applied in the cryptography domain to enhance efficiency and security of hyperchaotic encryption schemes, the biological operations and algebra operations in DNA encoding and DNA computing is the main reason of using DNA techniques [5]. In the field of encryption, many algorithms and auxiliary functions used to build cryptographic systems such as Message-Digest Algorithm 5 (MD5) which define as a one of cryptographic hash functions which processes variable-length or the message and convert into a fixed 128-bit output [6].

The rest of this paper is organized as follows. Section 2 gives review about previous works. In Section 3, contain the theoretical side of the techniques used in the proposal. Section 4 and 5 described the proposed authentication algorithm with evaluates of the algorithm. The last section concludes the

2. Related work

Many of the approach and techniques developed in this field, here the some of research is presents:

Pooja et al. [7] discussed the visual cryptography concept as split an image into number of shares which separately reveals no information about the original secret image. This technique uses the human visual system to perform the OR logical operation on the superimposed pixel of the shares. According to leaking, information about the original secret image is not meant from any given share of the secret image. The researcher considered this scheme insecure if the shape pattern or color of just a portion of the secret image can be recovered from any given share.

Fu C. et al. [6] developing the chaos-based image cipher based on permutation the plain text and change the positions of image pixels. The diffusion keystream generated of the cat map and Lorenz system. The hash functions helps to accelerate the diffusion process and has the avalanche property that lead to produced images different completely if a tiny difference between the original ones.

Sushko I. et al. [8] present the dynamical system based on piecewise linear map which known as the skew tent map. In particular, the skew tent map employ to describe the bifurcation structure of the parameter and the results is used to classify border collision bifurcations.

Yadav D. et al. [1] have proposed a uses the one-time password (OTP) in the e-commerce transactions to combat replay/eavesdropping attack which are considers types of attacks on network-connected computing environment or isolated computing setting proposed an increased security model of OTP system using ecc with fingerprint biometric.

3.1 Visual cryptography

Visual cryptography proposed by Naor and Shamir in, is a paradigm for cryptographic schemes that allows the decoding of concealed images without any cryptographic computation, it applied on black and white images as if the transparencies superpose with black and white pixels, the resulting pixel that our eyes see is black if at least one of the superposed pixels is black and is white if all the superposed pixels are white. Such a property can be rephrased as follows: the possible "state" for the pixels can be represented with a bit, using 0 for white and 1 for black, and the human visual systems performs an OR of the input pixels in order to reconstruct the secret pixels. This key property does not easily extend to colored pixels [9].

i. Error Diffusion Halftoning

There are several types of halftoning and the Error Diffusion Halftoning is most famous which is most commonly used in color visual cryptography. From algorithms which used for Error Diffusion Halftoning the Floyd Steinberg Halftoning Algorithm and Jarvis Halftoning Algorithm. Diffuses a error with Jarvis Halftoning Algorithm in the twelve neighboring cells instead of Diffuses an error in four cells with Floyd-Steinberg algorithm as display in figure (1). The comparison between Floyd Steinberg and Jarvis algorithms of error diffusion halftoning is done on the basis of parameters such as PSNR, SNR, Entropy and Correlation and in result the Jarvis kernel gives better visual quality [10].

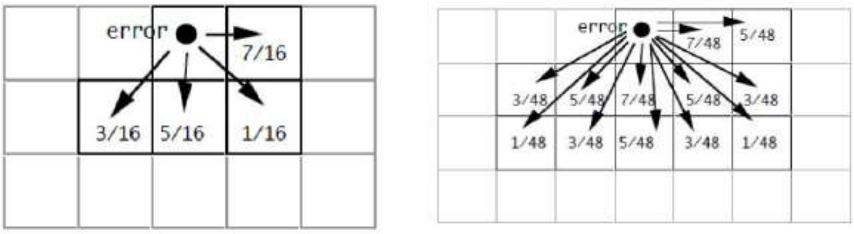

Figure1-(a)Floyd-Steinberg Halftoning(b)Jarvis Halftoning [10].

3.2 Generate Confusion Sequence

The confusion process can refer to the complex relationship between the key and the cipher text which means difficult to deduce the key even when an attacker knows the statistics[11] and from techniques which used to do confusion sequence:

i. Message Digest Algorithm

Message Digest Algorithm 5 (MD5) is refer as hash functions processing consists of four analogous stages,which are termed as rounds (sixteen 32-bit words) have three types of operations: bit-wise Boolean operation, modular addition, and cyclic shift operation, which is make MD5 very fast to break up the input message into blocks of 512-bit and operates on a 128-bit state, separated into four 32-bit words [12].

MD5 when generated 128 bits, can used only first 32 bits to generate d1, d2, d3, d4, each of which is a single byte. Only need to transform d1, d2, d3 and d4 from binary to decimal, The initial value of $x_0 \in (0,1)$ generate by eq.(1):

$$x_0 = \mathrm{mod}(d_1 \oplus d_2 \oplus d_3 \oplus d_4, 256)/255 \qquad \text{Eq.(1)}$$

ii. Piecewise Linear Chaotic Map

The asymmetric tent map is basically a distorted but still piecewise linear thus the data from this a map cannot be distinguished and generated by a first-order autoregressive process. Piecewise Linear Chaotic Maps (PWLCM) known as discrete dynamical systems and have one control parameter for all the values, since they posses a positive Lyapunov exponent for all the values of the control parameter[4].

On the other side the asymmetric tent map is defined a PWLCM as follows:

$$x_{i+1}=F_p(x_i) = \begin{cases} x_i/p, & x_i \in [0,p] \\ (1- x_i) / (1- p), & x_i \in (p,1] \end{cases} \qquad \text{Eq.(2)}$$

When $x_i \in [0, 1]$ and the parameter $p \in (0, 1)$, Eq. (2) owns positive Lyapunov exponent, the initial values of (x_0, p_0) can be served as keys [13].

3.3 Generate Diffusion Sequence

Diffusion defined as difficulty discover the key when compare the redundancy of the statistics of the plain text with the statistics of the cipher text [11] from techniques which do the diffusion:

i. Chen's Hyper-Chaotic System

The hyperchaotic system refer to as family of chaotic systems used as candidates to encryption the multimedia data which have more than one positive Lyapunov exponent [at least four] and have high efficiency, high security and high-capacity [14]. The hyperchaotic system generate the pseudorandom sequence with Chen's hyper-chaotic system which described as:

$$\begin{cases} t_1=a\,(t_2 - t_1)\,; \\ t_2= - t_1t_3 + d\,t_1 + ct_2 - t_4\,; \\ t_3= t_1t_2 - bt_3\,; \\ t_4=t_1 + k; \end{cases} \qquad \text{Eq.(3)}$$

In eq. (3), the system parameters control are a, b, c, d, k when a = 36, b = 3, c = 28, d = 16 and k is set as 0.2 [15].

ii. Runge-Kutta Method

Runge-Kutta method (RK) is widely used for simulating the solution of chaotic systems, from the past research and numerical comparisons the Runge-Kutta of orders 4 (RK4) can get better accuracy when employ to solve the chaotic system in different time steps than other methods which less reliability [16]. The most common Runge-Kutta method in use is of order four in difference-equation form, the following algorithim implements the Runge-Kutta method of order four [17].

Runge-Kutta (Order Four)

To approximate the solution of the initial-value problem

$$y` = f(t, y), \quad a \le t \le b, \quad y(a) = \alpha,$$

at (N + 1) equally spaced numbers in the interval [a, b]:

Input: endpoints a, b; integer N; initial condition α.

Output: approximation w to y at the (N + 1) values of t.

```
Step 1: Set h = (b − a)/N;
          t = a;
          w = α;
OUTPUT (t, w).
Step 2: For i = 1, 2, . . . , N do Steps 3–5.
Step 3:  Set K1 = hf (t, w);
              K2 = hf (t + h/2,w + K1/2);
              K3 = hf (t + h/2,w + K2/2);
              K4 = hf (t + h,w + K3).
Step 4: Set w = w + (K1 + 2K2 + 2K3 + K4)/6; (Compute wi.)
          t = a + ih. (Compute ti.)
Step 5: OUTPUT (t,w).
Step 6: STOP.
```

Where(ti, yi, h) is named an increment function, which is interpreted as the representative slope over interval. The estimate slope is used to extrapolate from an old value yi to a new value yi+1 over a distance h.This algorithm used to solve the Chen's chaotic system in order to find the values of t_1,t_2,t_3, and t_4 with the initial conditions (0.3 ,-0.4,1.2, 1).

iii. Deoxyribonucleic Acid Sequence

Deoxyribonucleic acid (DNA) is a type of molecules that are consist of four types of nucleotides. Adenine (A), Thymine (T), Cytosine (C) and Guanine (G). A, C, G and T in DNA sequence used to encode 00, 01, 10 and 11. A and T ,G and C are complementary just because in the binary system 0 and 1 are complementary, the DNA match rules are listed in following Table1[18]. DNA cryptography is defines as implementation tool used an information carrier and modern biological technology and appear as a new cryptographic area. DNA sequence based on rules and operation rules such as addition and subtraction (see Table-2 and Table-3) [19].

Table 1- Map rule of DNA sequence[18].

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
C	10	01	11	00	11	00	10	01
G	01	10	00	11	00	11	01	10
T	11	11	10	10	01	01	00	00

Table 2- Map of DNA addition [18].

+	T	A	C	G
T	C	G	T	A
A	G	C	A	T
C	T	A	C	G
G	A	T	G	C

Table 3-Map of DNA Subtraction [18].

	T	A	C	G

T	C	G	T	A
A	A	C	G	T
C	T	A	C	G
G	G	T	A	C

3.4 Information Entropy

In the image information, the information entropy is needed to express the degree of uncertainties in the system. The information entropy can measure the distribution of gray value in the image for an perfectly value the information entropy in random image is eight. The information entropy is describe as follows:

$$H(n) = -\sum_{i=0}^{L} P(n_i)\log_2 P(n_i) \qquad \text{Eq. (4)}$$

Where n_i is the i-th gray value for L level gray image, p(n_i) is the emergence probability of n_i [20].

4. The Proposed Algorithm

To increase the security of e-commerce applications, authentication system is proposed based on visual shares encapsulation by secret 4-D hyperchaotic sequence with encoded using DNA computing. In any e-commerce applications found two phases, the first phase is registration and the second phase is login, the proposed algorithm perform simulation for two phases the Figure-2 shown the flowchart of the proposed registration algorithm and the following explanation for the registration and login proposed algorithms.

The Proposed Registration Algorithm

Start: Customer choose the registration phase.

Output: Customer have secret share and image key on his email in addition to username and password which usually important to complete buying or sell transaction.

Processing:

Step-1: User entered his username and password with present his email then implement the authentication.

Step-2: Server request from user choose a color image from his computer to be the secret image.

Step-3: When the user loaded the secret image the server separate the secret image to additive color (Red, Green and blue) and each color matrix (Red, Green and blue) pass from through Jarvis halftone procedure.

Step-4: Generate two shares from each color channel by using visual cryptography.

Step-5: Generate Chen’s hyperchaotic when server choose unique initial values which consider a key for server to. Unique color image with any size selected from the server to be a key for user.

Step-6: The user key entered to MD5 to generate unique initial value.

Step-7: The unique initial value entered to PWLCM for produce a different number of DNA rules for each pixel.

Step-8: Convert decimal hyper-chaotic sequence into binary form then convert the six shares and Chen’s hyper-chaotic to vectors.

Step-9: Using the different DNA rules which output from step-7 to encode each element from six vectors and Chen’s hyper-chaotic.

Step-10: Implement DNA addition operation between the encoded hyper-chaotic with each one of six encode vectors.

Step-11: Using different DNA rules which output from step-7 to decode the six vectors from DNA form to binary form.

Step-12: Reship each encrypted vector to matrix and merge shares that generated from red, green and blue channel to build two cipher shares one for Customer and other for server.

Step-13: Send the customer share and image key to the user email and save the user’s information (username, password, server share, the initial values for hyper-chaotic)in server data base.

End.

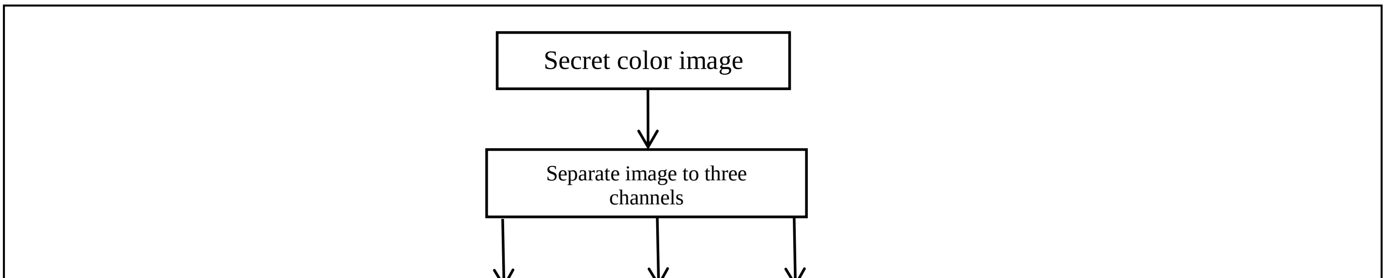

Figure 2-Block diagram for the proposed algorithm in Register Phase.

The Proposed Login Algorithm
Start: Customer choose the Login Phase and present his username.

Output: In secure way the user login to his account and he can deal with application in trust.
Processing:
Step-1: From server database, server retrieves the information for this customer if found such the second share and the initial values but if the customer not found the server is denied the login process.
Step-2: Server request from customer loaded user share and image key.
Step-3: When the customer loaded them the server generate Chen's hyper-chaotic sequence using the initial values and entered the image key to MD5 and PWLCA to produce a different number of DNA rules.
Step-4: Separation two shares into main colors (read, green, and blue) and convert six shares to vectors, with convert decimal hyper-chaotic into binary form then convert it to vector.
Step-5: Using different DNA rules to encode the six vectors and hyper-chaotic vector.
Step-6: Implement DNA subtraction operation between the encoded hyper-chaotic with each one of six encode vectors.
Step-7: Using different DNA rules to decode the six vectors from DNA form to binary form.
Step-8: Reship each encrypted vector to matrix and Perform OR operation between two shares which product from red channel in order rebuild red color channel and run this procedure also an Green and Blue shares.
Step-9: Merge three color channels to display the secret image to the user.
Step-10: The user entered his password if the image shown same the secret image but if display different image the site considered hacking attack.
End.

i. Generate Chen's Hyper-Chaotic Key Sequence

The hyperchaotic system generate the pseudorandom sequence based on four steps [20]:

1. Preiterated the hyperchaotic system N_0 times to increase the security and to eliminate the adverse effects so the first 1000 times are discard to avoid the transient effect and enhance initial value sensitivity.

2. After the iteration N_0 times, the system is iterated another m × n times and used j to show the index of iteration. In each iteration j, four state values { $t_1^j, t_2^j, t_3^j, t_4^j$ } is stored.

3. Every state value t^j_i is employ to generate $(s^a_i)^j \in [0,255]$ and $(s_i^b)^j \in [0,255]$ respectively which represent two key values. They are calculated by:

$$(s^a_i)^j = \bmod\left\{\left\lfloor\left\lfloor\left(\left|t_i^j\right| - \left\lfloor\left|t_i^j\right|\right\rfloor\right)\times 10^{15}\right\rfloor / 10^8\right\rfloor, 256\right\} \quad \text{Eq. (5)}$$

$$(s^b_i)^j = \bmod\left(\left\lfloor \bmod\left\{\left\lfloor\left(\left|t_i^j\right| - \left\lfloor\left|t_i^j\right|\right\rfloor\right)\times 10^{15}\right\rfloor, 10^8\right\}\right\rfloor, 256\right) \quad \text{Eq. (6)}$$

for i= 1,2,3,4

Where $\lfloor . \rfloor$ denotes flooring operation and mod (.) denotes the modulo operation. Two key values are merge to be a vector s^j by with Eq. (7)

$$s^j = [(s_1^a)^j, (s_2^a)^j, (s_3^a)^j, (s_4^a)^j, (s_1^b)^j, (s_2^b)^j, (s_3^b)^j, (s_4^b)^j] \quad \text{Eq. (7)}$$

4. Concatenated all sequences to obtain key(K)after the iteration is finish using Eq. (8)

$$K=[s^1, s^2, \ldots, s^{m\times n}]. \quad \text{Eq. (8)}$$

Denoted each element in k by k_i, $i \in [1; 8mn]$.

ii. Encryption Algorithm

The encryption procedure includes many steps to convert the secret image into encapsulation shares the following explain about these steps:

1. The algorithm proposed deals with the secret color image and the image key, the secret color image separated into main color channels and entered the key image to MD5.

2.When algorithm deals with color images and the color images consist from a set of three matrix{Red, Green, Blue} of size M × N, which contain of integer numbers in [0, 255] so the secret color plain image transformation into three images Red, Green and Blue then perform halftone on each image after that entered each image to visual cryptography to build two shares for each color channel.

3.convert six shares into vectors with size Y=M × N, so the original color image generate six vectors and generated the decimal 4-D hyper-chaotic sequence then transform it to binary vector.

4. When MD5 generated 128 bits and only the first 32 bits used to generate d1, d2, d3, d4, each of which is a single byte. The d1, d2, d3 and d4 transform from binary to decimal, then using eq.(1) to generate the unique initial value.

5.The PWLCM generate vector in size Y has numbers DNA rules based on initial value x_0 which generated from eq. (1). The complexity increased in this step were proposed using different DNA rules with each pixel for images{Red, Green, Blue}and hyper-chaotic sequence. For example, pixel with value 228 = (11100100)2 when represent in DNA rules that present in Table1 will be as: (TCGA) in Rule1, (TGCA) in Rule2, (CTAG) in Rule3, (GTAC) in Rule4, (CATG) in Rule5, (GATC) in Rule6, (ACGT) in Rule7 and (AGCT) in Rule 8. The PWLCM as Eq. (8):

$$X_{n+1}=F_p(X_n)= \begin{cases} X_n/p, & 0< X_n < p \\ (X_n - p) / (0.5- p), & p\leq X_n < 0.5 \\ F_p(1- X_n), & 0.5 \leq X_n <1 \end{cases} \qquad \text{Eq.(9)}$$

In our test the p appear as p = 0.25678900, each value from X entered to eq.(10) to generate number of DNA rules.

$$\text{Rule=floor}[x *8] \qquad \text{Eq.(10)}$$

6. Implement the DNA addition operation between Chen's hyper-chaotic sequence and each one of six vectors then use the DNA rules to decode six vectors.

7. Convert six vectors into images and merge Red, green and blue cipher images for each shares to build a two cipher color shares.

5. The Security Analysis

The proposed algorithm is tested on lena and peppers images as show in Figure (3, 4) with discuss in the following the security analysis of the proposed encryption algorithm.

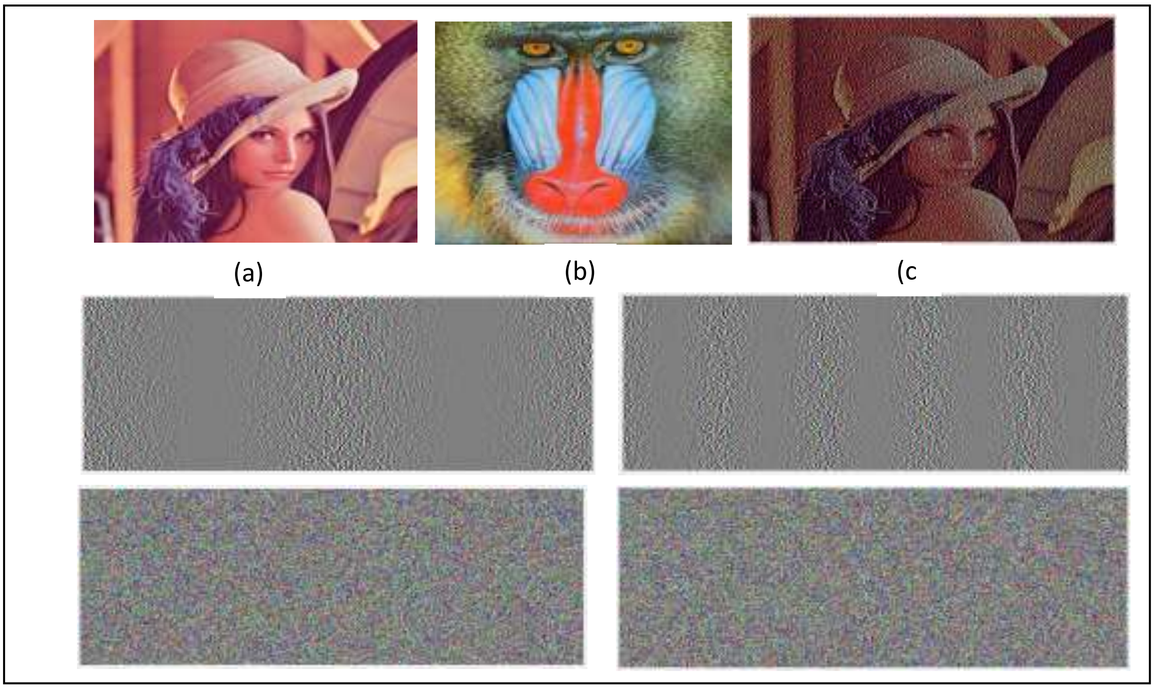

Figure 3- (a)The original Image (b)The Image Key (c)Reconstructed original Image .The second row represent two visual cryptography shares and the third row represent two shares after encapsulated .

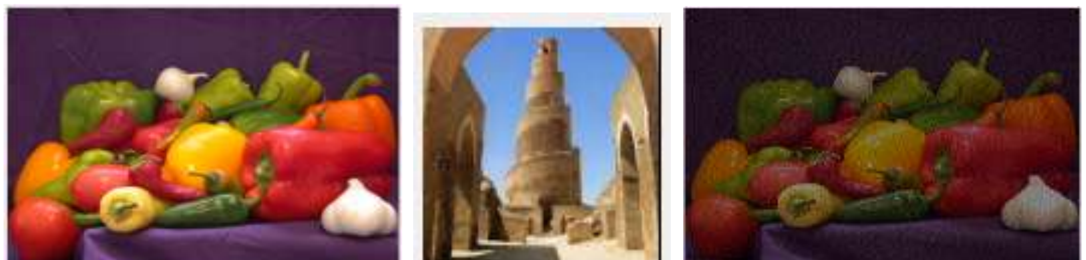

Figure 4- (a)The original Image (b)The Image Key (c)Reconstructed original Image .The second row represent two visual cryptography shares and the third row represent two shares after encapsulated .

i. Information entropy

A successful encryption algorithm must make the information entropy tend to eight, Table-4 show information entropy for channels (Red, Green, Blue) in proposed algorithm for two encrypted shares.

Table 4- Information Entropy for test images.

Test images	Shar1			Shar2		
	Red	Green	Blue	Red	Green	Blue
Lena	7.999616	7.999639	7.9996545	7.99967703	7.9996594	7.9996506
peppers	7.99953106	7.99951113	7.9995162	7.999503798	7.99952991	7.99955753

ii. Ability of Resisting Exhaustive Attack

In proposal algorithm, the secret key for server represent of the initial values of the Chen's hyper-chaotic system. Thus, t1, t2, t3, and t4 used as server key and supposed the t1 use value equal to 0.300000000000001 instead of 0.3 in order decode the encrypted shares that leads to generate different shares and because each variable from four initial values have sensitivity to change its value reach to 10^{15} so, the proposed algorithm employ this sensitivity with exploit the randomly property to generate new initial values for each new registration. In other word when new registration request the server randomly choose one variable [t1, t2, t3, and t4] to change its initial value based on employ the random number generator based on the current time with range 10^{13} to build new initial value.

iii. Histogram Analysis

Figure-5 show the histogram result when test lena image under the proposed algorithm and the histogram result for peppers image shown in Figure -6.

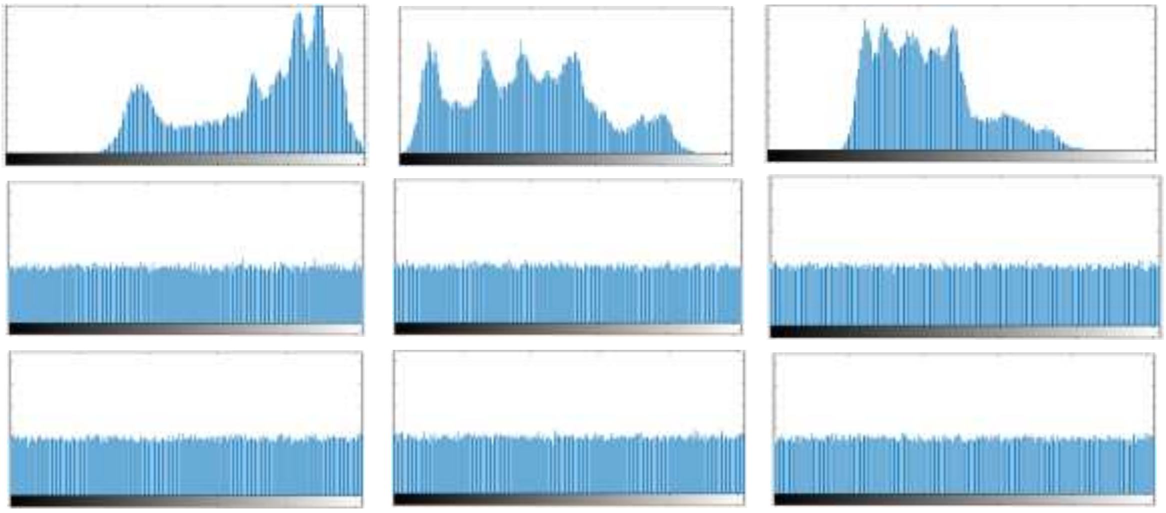

Figure 5-shows histograms of lena image {Red, Green and Blue} in first row and Red, Green and Blue histograms images for encrypted color shares in second and third rows.

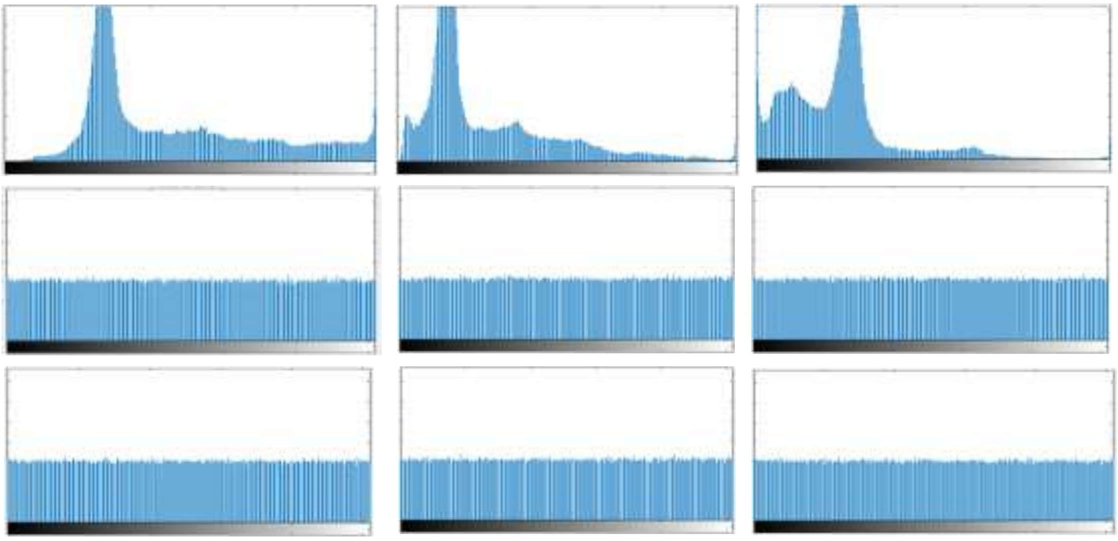

Figure 6- shows histograms of peppers image {Red, Green and Blue} in first row and Red, Green and Blue histograms images for encrypted color shares in second and third rows.

iv. Correlation Coefficient Analysis

The horizontal, vertical, and diagonal directions are checked of all adjacent pixels from the original image and the two encrypted shares. Table-5 display the rates correlation coefficients which denote that the pixels in two color shares are uncorrelated that make the proposed has well protected of resisting statistical attack.

Table 5-The correlations for proposed algorithm.

	Original			Share1			Share2		
	Red	Green	Blue	Red	Green	Blue	Red	Green	Blue
Lena									
Diagonal	0.94510	0.92932	0.90828	6.4844e-04	-5.3147e-04	0.001243	0.0016498	9.8055e-04	8.83848e-04
Horizontal	0.95262	0.93733	0.923600	8.9941e-04	-0.0020327	0.0018693	-0.0021301	0.00131426	-0.00134330
Vertical	0.97627	0.96981	0.954345	0.0033296	-0.0010695	-0.001687	6.2480e-04	0.00272702	-2.7921e-04
peppers									
Diagonal	0.98621	0.97899	0.970616	8.6195e-04	-0.001139	-1.4388e-04	5.3724e-04	0.0011929	-0.0011912
Horizontal	0.99413	0.99071	0.98657	0.0023183	0.001749	-0.001152	-0.001879	-5.3668e-05	6.0086e-04
Vertical	0.9896	0.98464	0.97595	-0.001607	0.002033	-9.5274e-04	0.001150	6.4163e-04	0.00334364

6. Conclusion

Online trust will continue be an important aspect of e-commerce even though both e-commerce and the Internet itself have evolved considerably over time. Establishing consumer trust in e-commerce presents a challenge for e-vendors and is a subject that generates continuous interest and research.

The proposed authentication system implemented to protect users from hacking attacks which in usually targeted the e-commerce applications to steal the private information from users and causing economic losses. The proposed algorithm depend on color visual cryptography and 4-D hyperchaotic system which is very sensitive for the initial condition which change for each new registration. DNA computing used to increased efficient the encapsulation to make the system resistant to online attacks. The proposed authentication system able to overcome on many attacks such as exhaustive and statistical with able to use this a system with each login application.

References

1. Yadav, D., Malwe, D., Rao, K. S., Kumari, P., Yadav, P. and Deshmukh, P. **2017.** Intensify the security of one time password using elliptic curve cryptography with fingerprint for e-commerce application. *International Journal of Engineering Science*, **7**(3): 5480-5482).
2. Bidgar, P. and Shahare, N. **2013.** Key based visual cryptography scheme using novel secret sharing technique with steganography. IOSR *Journal of Electronics and Communication Engineering* (IOSR-JECE), e-ISSN, 2278-2834. **8**(2): 11-18.
3. Liu, B., Martin, R. R., Huang, J. W., and Hu, S. M. **2014.** Structure aware visual cryptography. *In Computer Graphics Forum*, **33**(7): 141-150.
4. Rhouma, R., Arroyo, D., & Belghith, S. **2009.** A new color image cryptosystem based on a piecewise linear chaotic map. In Systems, Signals and Devices, 2009. SSD'09. 6th International Multi-Conference on (pp. 1-6). IEEE.
5. Wang, X., and Chen, D. **2013.** *A parallel encryption algorithm based on piecewise linear chaotic map. Mathematical Problems in Engineering*, Hindawi Publishing Corporation.
6. Fu, C., Bian, O., Jiang, H. Y., Ge, L. H., & Ma, H. F. **2016**. A new chaos-based image cipher using a hash function. In Computer and Information Science (ICIS), 2016 IEEE/ACIS 15th International Conference on (pp. 1-9). IEEE.
7. Pooja,& Lalitha,Y. (2014, June).Non Expanded Visual Cryptography for Color Images using Pseudo-Randomized Authentication. *International Journal of Engineering Research and Development*, **10**(6).
8. Sushko, I., Avrutin, V., & Gardini, L. **2016.** Bifurcation structure in the skew tent map and its application as a border collision normal form. *Journal of Difference Equations and Applications*, **22**(8): 1040-1087.
9. Cimato, S., & Yang, C. N. (Eds.). **2017.** *Visual cryptography and secret image sharing*. CRC press.
10. Nikate, P. M., & Mujawar, I. I. **2015**. Performance Evaluation of Floyd Steinberg Halftoning and Jarvis Haltonong Algorithms in Visual Cryptography. *International journal of Innovations in Engineering and Technology* (IJIET). **5**(1): 336-342.

11. Stallings, W. **2016**. *Cryptography and network security: Principles and practice. Pearson*.

12. Azad, S., & Pathan, A. S. K. (Eds.). ***2014***. *Practical Cryptography: Algorithms and Implementations Using C++*. CRC Press.

13. Kadir, A., Hamdulla, A., & Guo, W. Q. **2014**. Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. *Optik-International Journal for Light and Electron Optics*, **125**(5): 1671-1675.

14. Chen, A., Lu, J., Lü, J., Yu, S. **2006**. Generating hyperchaotic Lü attractor via state feedback control. Physica A: *Stat. Mech. Appl.* **364**(C): 103–110.

15. Zheng, W., Wang, F. Y., & Wang, K. **2017**. An ACP-based Approach to Color Image Encryption Using DNA Sequence Operation and Hyper-chaotic System.. 2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC).pp.461- 466

16. Mehdi, S. A., & Kareem, R. S. **2017**. Using Fourth-Order Runge-Kutta Method to Solve Lü Chaotic System. American Journal of Engineering Research (AJER), **6** (1): 72-77.

17. Richard, L.,& J. Douglas, Faires. **2011**. *Numerical analysis*.9th ed.

18. Enayatifar, R., Abdullah, A. H., & Isnin, I. F. **2014**. Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Optics and Lasers in Engineering* **56**: 83-93.

19. Niyat, A. Y., Hei, R. M. H., & Jahan, M. V. A. (2015, October). RGB image encryption algorithm based on DNA sequence operation and hyper-chaotic system. Conference Paper.

20. Zhan, K., Wei, D., Shi, J., & Yu, J. (2017). Cross-utilizing hyperchaotic and DNA sequences for image encryption. *Journal of Electronic Imaging*, **26**(1): 013021.