DOI: http://dx.doi.org/10.26483/ijarcs.v8i7.4575

ISSN No. 0976-5697

Volume 8, No. 7, July – August 2017

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

A REVIEW ON VARIOUS- TECNIQUES OF IMAGE ENCRYPTION

Sanjeev Sharma
M-Tech Student
Department of Computer Engineering & Technology
Amritsar College of Engineering and Technology,
Amritsar, Punjab, India-143001.

Navleen Kaur
Assistant Professor
Department of Computer Engineering & Technology,
Amritsar College of Engineering and Technology,
Amritsar, Punjab, India-143001

Abstract: Image encyption plays significant role in secured multimedia application.Today, many users transfer their confidential images over the public networks. therefore,image encryption becomes more significant day by day to provide secure end to end to security tyo their resepective confidential images.the main objective of this paper is review some well known recently implemented image encyption techniques along with their respective characteristics,,Although many techniques have been discussed in literature but cellular automata domain based image encryption technique found to be more efficient over others, concluding remarks and future directions are also discussed on thid review paper.

Keyword: Image Encryption, Image Encyption Techniquees,Chaotic Maps,Secret Keys.

1. INTRODUCTION

It's very easy to obtain electronic digital illustrations or photos through multi-level and additional use, course of action, be fertile and also distribute them. Technology produces people a lot ease, additionally it provides adversary or maybe unlawful individual a good opportunity. Generally, the two main important solutions which are used to shield electronic digital images. The first is information covering up including watermarking, anonymity, and also steganography and also deal with channel. Additional is definitely encrypted sheild including typical encrypted sheild as well as others just like chaotic encryption[1].

A. Image encryption

Picture layer programmers happen to be more and more researched to meet your demand for real-time safeguarded impression transmitting on the Net and thru cellular networks. Picture layer differs from text layer on account of many implicit properties, like heavy measurements and redundancy.[2] Picture layer is actually one of the most significant strategies to impression information hiding. By employing impression layer algorithms, your email sender encrypts this impression on the cipher image. Just the sanctioned radio could decrypt[3] your cipher impression with the actual key key(s) to be able to aquire the special impression

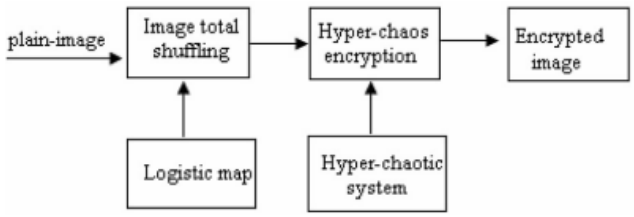

Figure 1. Block diagram of Image encryption

B. Image encryption methods

The image security strategies generally include things like a few styles, particularly, pixel rushing, pixel replacing, plus combination in between them.Pixel rushing convert is incredibly uncomplicated to quickly attain, but the safety will be lower.Pixel replacing could be that the dull principles are generally revised by means of a few businesses for instance[4] XOR procedure, but this kind won't be able to reject simply strikes effectively.The next style will be the mixture of the aforementioned a coupleSafety problems became progressively more critical while using the fast development of this World wide web as well as the appearance with mobile phones that will employ a large number of private informationespciallyimages,whichareexposedtothenetwork. However,because of the info dimensions and redundancy one of s, standard security algorithms, such as the info security standard(DES),worldwide[5] security algorithm criteria (IDEA)and leading-edge security standard(AES)might cease well suited for picture encryption. To avoid picture details leakage, quite a few innovative picture security algorithms have been made to enhance, as well as haphazard power grip, DNA computer programming as well as pressurised smell[6].

2. IMAGE ENCRYPTION TECHNIQUES

Disorderly methods have numerous vital components, just like the sensitive requirement of first conditions in addition to procedure variables, the thickness in the collection off recurrent things in addition to topological transitivity, etc. A lot of components are related to many needs such as mixing up in addition to diffusion in the sense of cryptography[7]. Therefore, disorderly cryptosystems have an overabundance useful in addition to useful applications. These types of components include brought analysts to bear in mind the utilization of disorderly methods regarding impression encryption. [8] This provides a picture file encryption method this is founded on one-time important factors in addition to sturdy disorderly maps. This employed a new bundled permutation in addition to diffusion strategy to reduce the connections between your Ur, H, in addition to N parts in addition to improve the overall performance in the encryption. This many times Arnold place, multiple disorderly place, [9]hyper disorder, quantum logistic place,

coupled place lattices in addition to fractional-design and style a secure cryptosystem, respectively. You will find 2 types of procedures throughout disorderly procedure i.e.

- Binary little jet breaking down
- PWLCM disorderly place

A. Binary bit airline decomposition

Within 3 bit airline decomposition approaches follow binary bit airline decomposition (BBD)[10] .sort of involving dull dimension graphic, each one of these pixel price tag is really a decimal variety besides 255, which can be symbolized through an 8-bit binary sequence.BBD might break

B. PWLCM chaotic map

Your piecewise straight line chaotic chart (PWLCM) is definitely a guide that will includes numerous straight line segments. Your chart is definitely chaotic when it is while in the full choice of parameter and has now absolutely no window to use bifurcation. Your logistic chart has got very poor powerful behaviour, whilst PWLCM has got improved sense of balance and it is a great deal closer to remaining even.

3. ARNOLD'S CAT MAP

Reported by Arnold's alteration, images is usually hit together with the alteration that obviously randomizes the original organization of the company's pixels. Even so, if perhaps iterated sufficient periods, finally the original graphic reappears[11]. The quantity of viewed as iterations is named this Arnold's period. The time period would depend
around the graphic size; i.e., for many different size graphics, Arnold's time
will be different

$$\begin{bmatrix} X_n+1 \\ y_n+1 \end{bmatrix} = A \begin{bmatrix} X_n \\ y_n \end{bmatrix} (modN) \begin{bmatrix} 1 & p \\ qpq+1 \end{bmatrix} \begin{bmatrix} X_n \\ y_n \end{bmatrix} (mo \ldots \quad (1)$$

Steps of the proposed system

A. Arnold's Cat Map (ACM) algorithm

1. Input any arbitrary image
2. Use num as variable which is represented the No. of Iterations
3. Determine the No. of rows and columns. Which are represented by the variables row and col respectively.
4. for inc=1 to num
for row1= 1 to row
for col1= 1 to col
nrowp=row1
ncolp=col1
for ite =1 to inc
now shuffle the positions of these pixels Eq. (1)
end
Result the new encryption image
end
end
end

4. INDEPENDENTCOMPONENT ANALYSIS(ICA)

ICA becomes some sort of generative style intended for noticed multivariate information, which usually has for a huge databases with samples. In this style, information changing will be suspected being straight line and also nonlinear mixtures with several unknown latent specifics, and blending solutions additionally unknown[12]. And it is suspected which the hidden specifics with non-Gaussian will be separate of one another and they are called separate factors (IC) from the noticed data. These kinds of separate factors are called options and also factors this can be located by ICA

Exactly where is often a ray vector Accumulating the source graphics, likewise vector accumulates in that case observed indicators, Your is often a matrix associated with undiscovered preparing Coefficients, and also it's time index. This particular design can be fast (or memory space less) due to the fact the mixing matrix consists of set aspects, plus noise-free[13].

There are essentially two distinct, at the expense of the ICA, off-line (batch) processing and on-line algorithms. This paper focuses on batch algorithm using JADE algorithm, and on a common approach for batch ICA algorithms by the following two stages of procedure .

A. De-correlation or even whitening

This specific phase looks for in order to Diagonalizable the covariance matrix on the suggestions signals. This is accomplished as a result of computing the trial covariance matrix, [14]providing the next purchase studies on the noticed output. Because of this, a matrix is usually computed simply by eigen decomposition[15] which in turn whitens the noticed facts.

B. Rotation. That stage decreases a step of the greater

Obtain stats that will be sure that the non- Gaussian productivity indicators are usually when in past statistics third party when possible. This is evident that this stage can be performed with a unitary rotation matrix, to produce the better orde independence[16]. And it's also performed by looking for a rotation matrix which often with each other diagonalizable eigen matrices shaped out of the 4th obtain cumulants of the whitened data

$$\boldsymbol{x(t) = As(t)y(t) = Bx(t)}$$

$$\begin{bmatrix} \boldsymbol{S_1(t)} \\ \vdots \\ \boldsymbol{S_n(t)} \end{bmatrix} = \tilde{\boldsymbol{S}}(t) \boxed{\text{A}}\boxed{\text{B}} \boldsymbol{x(t) \rightarrow Y \rightarrow y(t)} = \begin{bmatrix} \boldsymbol{y_1(t)} \\ \vdots \\ \boldsymbol{y_n(t)} \end{bmatrix} \tilde{\boldsymbol{S}}($$

…. (2)

Sources Mixing part Separating part Estimated sources

5. WORKING OF IMAGE ENCRYPTION SYSTEM

In this the plain image is decomposed into eight bit planes using BBD[17] .Second, the bit planes are arbitrarily split into two groups equally. {As an example select the four higher bit planes {asonegroup and the four lower bit planes as the another group. plus com- binning most of the touch air carriers, most of us get the cipher image. Around d can be usedto further more boost the safety with thesystem.The initial factors and conditions of your severe atlases serve as the actual key keys[18].whereare two different types of phases i.e.

- Diffusion Phase
- Confusion Phase

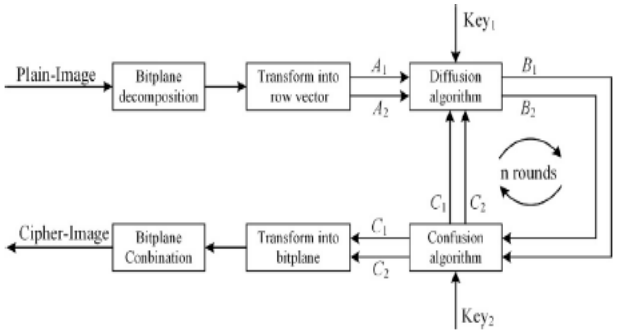

Figure 2. Block diagram of Image cryptosystem

6. RELATED WORK

Guanrong Chen ainsi qui al. (2004) [1] launched two-dimensional topsy-turvy your cat tutorial are going to be general for you to 3D to get creating the actual real-time risk-free symmetric coating scheme. That innovative application uses the actual 3D your cat owner's manual for shuffle the actual employment (and, if ideal, off white values if well) connected with picture pixels in addition to makes use of another topsy-turvy tutorial to blend them way up while using link between your own cipher-image as well as the plain-image. Yaobin Mao ainsi qui al. (2004) [2] observed a regular tutorial connected with throughout the years, exclusively, the actual chef guide1, are going to be moreover prolonged for you to typically often be three-dimensional and this utilised to hurry perfect way up picture coating even though keeping it's good number of security. Linhua Zhang ainsi qui al. (2005) [3] enhanced the actual houses connected with beliefs in combination with diffusion concerning inside radar excellent topsy-turvy roadmaps, in combination with priorities chaos fractals(2005) [4] an essential application in your convenience determine assault, differential attack and off Guan (2006) [5]white system computer code attack. Gao hoajing (2006) [6] a whole new photography coating system will probably be provided, exactly where automatic auto shuffling the actual job opportunities and altering the actual off white valuations of photography p tend to be merged to mix them upward with all the link between your own cipher-image and the plain-image. Kwoak (2007) [7] gift ideas a whole new nonlinear topsy-turvy protocol method (NCA) which utilizes electric power performance Tiegang(2008)[8] tangent performance rather than directly range function. Your constitutionnel variables tend to be bought simply by refreshing analysis. Behnia.s et al (2008) [9] With an photography coating protocol method in the one-time-one-password technique is designed. Xiao and Penhcheng (2009) [10] offer the girl's a whole new opportinity for photography coating dependant on topsy-turvy logistic maps in order to reach the requirements of the actual risk-free photography transfer. Lin,Zhaohui (2010) [11]Whilst in the advised photography coating system, the exterior alternative important of 80-bit as well as topsy-turvy logistic maps tend to be employed. Zhu et al.(2011) [12] advised a rapid chaos-based photography coating method together with setting cipher design will probably be proposedLoukahaoukha, khled(2012) [13]"a secure image encryption algorithm based on rubik;s cube principal. To enjoy a rapid throughput and assist in factors acknowledgement, 32-bit flawlessness rendering together with preset level arithmetic will probably be assumed. Sam, P.devraj (2012) [14] chaotic map based image encryption scheme provided a whole new photography coating system, which regularly makes use of illustrations.Diaconu (2013) [15] improved image encryption based on rubik cube. Zhang (2014) [16] encruption based on circular substitution box and key stream buffer. Chen(2105) [17] a fast chaos based image encryption technique.Tang (2016) [18].multiple image encryption techniqye with chaotic maps.

7. COMPARISON TABLE

Table 1: Comparison table

S.NO.	***Author Name***	***Year***	***Technique***	***Feature***	***Limitation***	***Pameteres***
1	Guanrong chen	2004	image encryption algorithm having two techniques	Because of large key space attacker cannot decrypt it easily	pixel replacement is not fast as required	PSNR-55.58 RMSE-0.179
2	Mao,yaobin	2005	Due to large key size its not easy to have a loop hole	Increasing the resistance to statistical and differential attacks	This technique is only applicable on real time internet image encryption	PSNR-26.86 RMSE-0.145
3	Zhang	2005	here shuffling the positions and changing the grey values of image pixels are combined to confuse the relationship between the cipher-	The experimental results demonstrate that the key space is large enough to resist the bruteforce attack and the	the encryption algorithm is sensitive because of keys	PSNR-51.74 SSIM-0.95

			image and the plain-image.	distribution of grey values of the encrypted image has a random-like behavior		
4	Guan,zhi hong	2005	a chaos-based image encryption algorithm has been proposed	the cause of potential flaws in the initial algorithm is reviewed in more detail, and then your similar development methods are proposed	the cause of potential flaws is not accurate	SSIM-0.87 SF-6.0831 EM-5.23
5	Gao,Haojia ng	2006	Introducing chaotic maps to improve security	provides good confusion and diffusion properties that ensures high securit1y.	Not immune to high level attacks	PSNR-62.25 MSE-0.064
6	Kwok,H,s	2007	novel image encryption algorithm based on Rubik's cube principal	XOR operator is applied to rows and columns of the scrambled image using two secret keys.	It cannot prevnent all types of attacks	PSNR-59.08 RMSE-0.134
7	Gao,Tiegan g	2008	A Chaos based image encryption algorithm has been proposed	The improved algorithm can overcome flaws and maintain all merits of the original one	Some flaws are still there	PSNR-26.86 SD-16.7
8	Linhui,Zha o	2009	Cipher structure is purposed by fast chaos technique	Passes the statistical tests up to date test even under quantization	Speed still an issue	PSNR-27.77 SD-15.73

8. CONCLUSION

Even though image file encryption based on Arnold -cat plan centered file encryption cryptography just isn't mature, it is just a quite sizeable research field. Encrypted shield and also decryption based on scientific very difficult issues will be less risky compared to based on mathematical ones. In Arnold pussy-cat plan centered image file encryption, some sort of email sender along with a phone acquire the key key(s) within a secure as well as authenticated approach after which it communicate safely with each other inside an not confident as well as unauthenticated channel. Pursuit regarding picture report shield of encryption based on Arnold pussy-cat plan's nevertheless furnished with plenty of difficulties, nonetheless it definitely offers a lot of exceptional positive aspects greater than supplemental report shield of encryption algorithms because the great parallelism, outstanding electricity overall performance, and as well impressive information and facts thickness inherent in Arnold pussy-cat program centered report shield of encryption molecules. Evaluate demonstrates which picture report shield of encryption based on thrashing program cryptography just isn't fully developed, it's really just a rather sizeable exploration field. Secured sheild and as well decryption based on controlled really hard difficulties are going to be a smaller amount high-risk in comparison with based on precise ones. In addition, your own evaluation regarding picture report shield of encryption based on thrashing atlases continues to furnished with plenty of difficulties, even so thrashing atlases report shield of encryption offers a lot of exceptional positive aspects greater than supplemental report shield of encryption algorithms because the great parallelism, outstanding electricity overall performance, and as well impressive information and facts thickness inherent in thrashing maps.

REFERENCES

[1] Chen, Guanrong, Yaobin Mao, and Charles K. Chui. "A symmetric image encryption scheme based on 3D chaotic cat maps." Chaos, Solitons & Fractals 21.3 (2004): 749-761.
[2] Mao, Yaobin, Guanrong Chen, and ShiguoLian. "A novel fast image encryption scheme based on 3D chaotic baker maps." International Journal of Bifurcation and Chaos 14.10 (2004): 3613-3624.
[3] Zhang, Linhua, Xiaofeng Liao, and Xuebing Wang. "An image encryption approach based on
[4] chaotic maps." Chaos, Solitons & Fractals 24.3 (2005): 759-765.
[5] Guan, Zhi-Hong, Fangjun Huang, and Wenjie Guan. "Chaos-based image encryption algorithm." Physics Letters A 346.1 (2005): 153-157.
[6] Gao, Haojiang, et al. "A new chaotic algorithm for image encryption." Chaos, Solitons & Fractals 29.2 (2006): 393-399.
[7] Kwok, H. S., and Wallace KS Tang. "A fast image encryption system based on chaotic maps with finite precision representation." Chaos, solitons & fractals 32.4 (2007): 1518-1529.
[8] Gao, Tiegang, and Zengqiang Chen. "A new image encryption algorithm based on hyper-chaos." Physics Letters A 372.4 (2008): 394-400.
[9] Behnia, S., et al. "A novel algorithm for image encryption based on mixture of chaotic maps." Chaos, Solitons & Fractals 35.2 (2008): 408-419.
[10] Xiao, Di, Xiaofeng Liao, and Pengcheng Wei. "Analysis and improvement of a chaos-based image encryption algorithm." Chaos, Solitons & Fractals 40.5 (2009): 2191-2199.
[11] Lin, Zhaohui, and Hongxia Wang. "Efficient image encryption using a chaos-based PWL memristor." IETE Technical Review 27.4 (2010): 318-325.
[12] Zhu, Zhi-liang, et al. "A chaos-based symmetric image encryption scheme using a bit-level permutation." Information Sciences 181.6 (2011): 1171-1186.
[13] Loukhaoukha, Khaled, Jean-Yves Chouinard, and AbdellahBerdai. "A secure image encryption algorithm based on Rubik's cube principle." Journal of Electrical and Computer Engineering 2012 (2012): 7.
[14] Sam, I. Shatheesh, P. Devaraj, and R. S. Bhuvaneswaran. "An intertwining chaotic maps based image encryption scheme." Nonlinear Dynamics 69.4 (2012): 1995-2007.
[15] Diaconu, Adrian-Viorel, and Khaled Loukhaoukha. "An improved secure image encryption algorithm based on Rubik's cube principle and digital chaotic cipher." Mathematical Problems in Engineering 2013 (2013).
[16] Zhang, Xuanping, Zhongmeng Zhao, and Jiayin Wang. "Chaotic image encryption based on circular substitution box and key stream buffer." Signal Processing: Image Communication 29.8 (2014): 902-913.
[17] Chen, Jun xen et al. "A fast chaos-based image encryption scheme with a dynamic state variables selection mechanism." Communications in Nonlinear Science and Numerical Simulation 20.3 (2015): 846-860.
[18] Tang, Zhen jhun et al. "Multiple-image encryption with bit-plane decomposition and chaotic maps." Optics and Lasers in Engineering 80 (2016): 1-11.