Volume 3, Issue 8, August 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Technical Review on Symmetric Key Cryptography Algorithm on Images

Niraj Kumar, Prof. Sanjay Agrawal
Department of Computer Engineering and Application
National Institute of Technical Teacher
Training and Research, Bhopal , India

Abstract: It is well-known that images are different from texts in many aspects, such as highly correlated, redundancy and the characteristics in 2D pixel matrix. Cryptography algorithm for image is not so easy. RES, AES, DES are not suitable for color images, which are 2D arrays of data. As a result, the methods of conventional encryption cannot be applied to images. The network is currently used for carrying personal information as well as financial data. Thus, it is necessary to secure the network, in order that unauthorized person cannot access personal information. Cryptography is used for protecting data during network communication. Encrypting information in transfer helps to secure it from hackers, because it is difficult to physically secure all access to network cannel. Standards cryptographic hardware and software are used to perform encryption and decryption. There are many cryptographic algorithms which are being used to secure data including images but all of them have some advantages and disadvantages. So there is need to develop a strong cryptography algorithm for securing the image while transferring. Graphical data is complicated in comparison with other data like text, so technique of securing them also will be difficult.

Keywords- Cryptosystem, Symmetric key encryption, Encryption, Images cryptography, Decryption.

I. INTRODUCTION

In the current world that we tend to board, of speedy growing technology, and particularly trust on the net for our daily spirited hood (Banking, shopping, diversion, news), and conjointly with current crimes (Identity-theft, hacking, spyware), PC security is turning into a lot of and a lot of necessities. By “computer security”, we regularly visit addressing 3 necessary aspects of a computer-related system: Confidentiality, integrity and convenience. Encoding clearly addresses the necessity for confidentiality of knowledge, each in storage and transmission. Widespread application of multimedia system technology and progressively transmission ability of network step by step leads United States to accumulate info directly and clearly through pictures [1, 2, 3]. Substitution cipher is one among the fundamental parts of classical ciphers. A substitution cipher could be a methodology of encoding by that unit of plain image area unit substituted with Cipher image in keeping with an everyday system; the units could also be single letters (the most common), triplets of letters, pairs of letters, mixtures of the higher than, then forth. The receiver deciphers the text by playacting associate inverse substitution. The units of the plain image area unit preserved within the same sequence as within the Cipher image, however the units themselves are a unit altered. There are a unit variety of various kinds of substitution cipher. If the cipher operates on particular inscription, it's termed an easy substitution cipher; a cipher that operates on larger teams of letters is termed poly-graphic cipher. A mono alphabetic cipher uses fastened substitution over the whole message, whereas a poly alphabetic cipher uses a variety of substitutions at totally different times within the message — like with homophones, wherever a unit from the plain image is mapped to 1 of many potentialities within the Cipher image [4]. Some intrinsic options of pictures, like bulk information capability and the high correlation between pixels, ancient coding algorithms like DES, plan and RSA aren't appropriate for sensible image coding, particularly beneath the situation of on-line communications [5]. The chaos-based coding has steered a brand new and economical thanks to subsume the unmanageable downside of quick and extremely secure image coding. When Matthews planned the chaotic coding algorithmic rule in 1989 [6], increasing researches of image coding technology supports chaotic systems [7,8]. Recently there are several papers on chaotic coding theme [9-18]. Chaos theory has been used since Nineteen Seventies in many various analytical areas, like physics, arithmetic, engineering, biology, etc. Since Nineteen Nineties, several researchers have detected that there exists the shut relationship between chaos and cryptography [19,20]; several properties of chaotic systems have their corresponding counterparts in ancient cryptosystems. Chaotic systems have many important options favorable to secure communications, like stochasticity, sensitivity to initial conditions, management parameters and random-like behavior, which may be connected with some park et al. [10] Extended the idea of their document cipher to image coding by mistreatment 2 supply maps [11].

II. TECHNICAL REVIEW:

According to Amir- Masud Eftekhari-Moghadam Sahar Mazloom, Image cryptography is somehow completely different from text encryption attributable to some natural options of image like mass knowledge capability and the high correlation between pixels, that area unit usually tough to handle by typical ways. The exceptional standard properties of the chaotic maps like sensitivity to initial conditions and random-like behaviour have attracted the eye of cryptographers to develop new cryptography algorithms. This paper proposes a brand new cruciate image cipher supported the wide used confusion–diffusion design that utilizes the chaotic second customary map and 1D provision map. It's specifically designed for the color pictures, that area unit 3D arrays of knowledge streams. We have a tendency to like the chaotic customary map to Baker and Cat maps since the key house of the chaotic customary map is massive enough as compared to the Baker and Cat maps, that makes the brute-force attack unworkable. The initial conditions and system parameters of the chaotic maps represent the key key of the formula. Two additional enhance the protection, the management parameters employed in the confusion stage and therefore the key stream used for diffusion stage area unit distinct in numerous rounds and associated with the plain-image. These management parameters area units generated by a Tent map. For obtaining higher security and better complexness, this theme employs 2 types of diffusion processes particularly the horizontal and vertical diffusions that area unit completed by admixture the properties of horizontally and vertically adjacent pixels employing a provision map, severally. The results of many experiments, mutually with the foremost vital ones like key house analysis, key sensitivity check, applied mathematics analysis, and visual check by histograms of encrypted images, the correlation coefficients of adjacent pixels, demonstrate the satisfactory security and potency of the planned image cryptography theme for time period image cryptography and transmission [21].

In recent years, the chaos primarily based cryptological algorithms have instructed some new and economical ways that develop secure image secret writing techniques. During this communication, we tend to propose a replacement approach for image secret writing supported chaotic logistical maps so as to ful fill the wants of the secure image transfer. Within the projected image secret writing them, AN external secret key of 80-bit and 2 chaotic logistical maps area unit utilized. The initial conditions of the each logistical maps area unit derived victimization the external secret key by providing totally different weighted to any or all its bits. Further, within the projected secret writing method, eight differing kinds of operations area unit want to code the peals of a picture and that one in every of them are going to be used for a selected pixel is determined by the result of the logistic map. To form the cipher additional sturdy against any attack, the key secret is changed once encrypting every block of sixteen pixels of the image. The results of many experiments, applied math Analysis and key sensitivity tests show that the projected image secret writing theme provides an economical and secure manner for a period of time image secret writing and transmission [23].

In this paper authors stress on info security is a very important issue. Today’s secret writing technologies are often derived back to the earliest ciphers, and have fully grown as a result of evolution. The primary ciphers were hacking, so we need a new stronger cipher emerged. Code breakers set to figure on these and eventually found flaws, forcing cryptographers to create higher ciphers so on. Hill Cipher is one in every of the foremost notable bilaterally symmetrical cryptosystem that may be wanted to defend info from unauthorized access. Hill cipher could be a medical instrument substitution cipher supported algebra. It had been the primary medical instrument cipher that was sensible to work on quite 3 symbols promptly, Hill Cipher has several blessings in encoding. First, it's proof against the letter frequency analysis. It is also terribly straightforward since it uses matrix operation. Finally, it's high speed and high output. However, noninvertible key matrix over Z_{mis} the most disadvantage of Hill Cipher, as a result of a few of the matrices has inverses over Z_m. This suggests that the encrypted text cannot be decrypted. Moreover, Hill cipher formula cannot encode pictures that contain giant areas of one colour. Thus, it doesn't hide all options of the image that reveals patterns within the plaintext. Moreover, it is often simply broken with an identified plain image attack revealing weak security. The target of this paper is to encode a picture employing a totally different technique from the standard one. During this paper, a completely unique secret writing technique has been planned that they name H-S-X (Hill-Shift-XOR) secret writing. The theme is comparatively slow however quite strong reliable technique wherever cryptography is kind of troublesome. It additionally injects additional diffusion and confusion that area unit the 2 vital attributes of a strong secret writing technique. A comparative study of the planned secret writing theme and therefore the existing Hill cipher theme is formed. The output encrypted pictures reveal that the planned technique is kind of reliable [22].

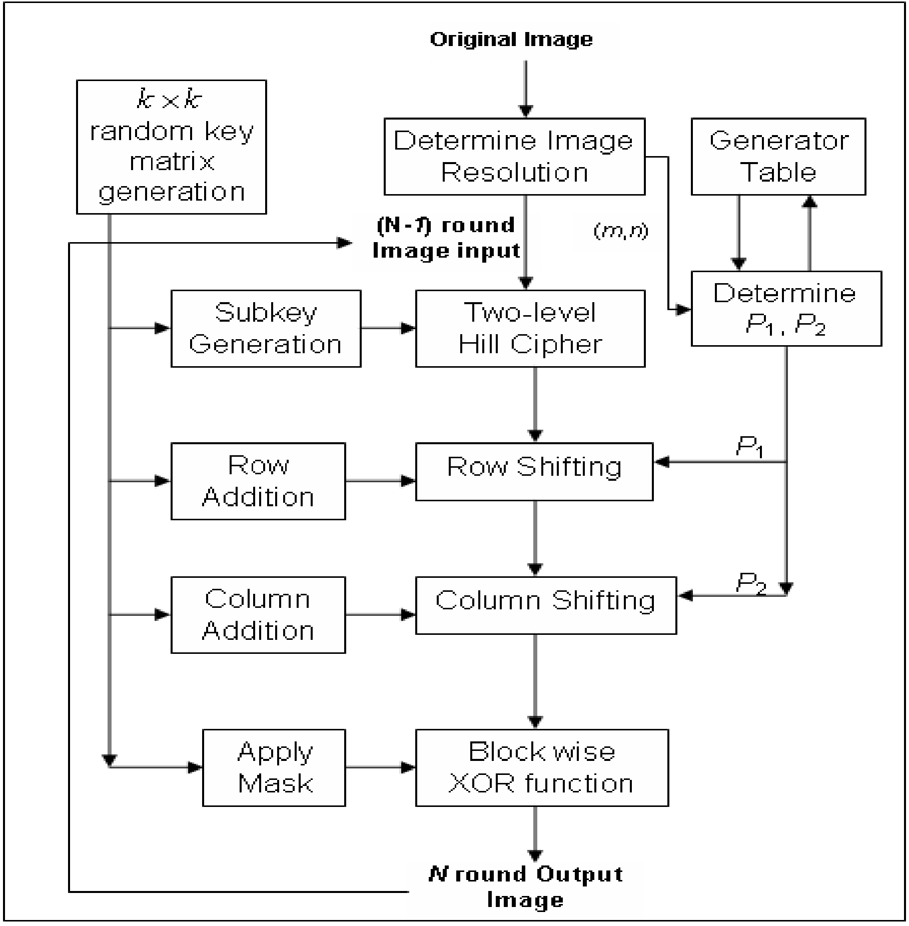

Figure 2.3. The block diagram for proposed H-S-X algorithm [22].

According to Linhua Zhang, Xiaofeng Liao, Xuebing Wang, image area unit completely different from texts in several aspects, like extremely redundancy and correlation, the native structure and also the characteristics of amplitude–frequency. As a result, the ways of typical secret writing cannot be applied to photographs. In this paper author, tend to improve the properties of confusion and diffusion in terms of distinct exponential chaotic maps, and style a key theme for the resistance to datum attack, differential attack and gray code attack. Experimental and theoretical results additionally show that our theme is economical and extremely secure. In this paper authors resistance to differential attack and linear attack, they tend to propose the quite smart datum properties of distinct exponential chaotic maps, In virtue of them, they tend to style a spatial S-box, and then, they tend to style a key theme for the resistance to datum attack and gray code attack. In fact, the theme will resist to the error operate attack (EFA) that be thought to be an awfully effective attack. Finally, Experimental and diagnostic results show that theme is economical and extremely secure [24].

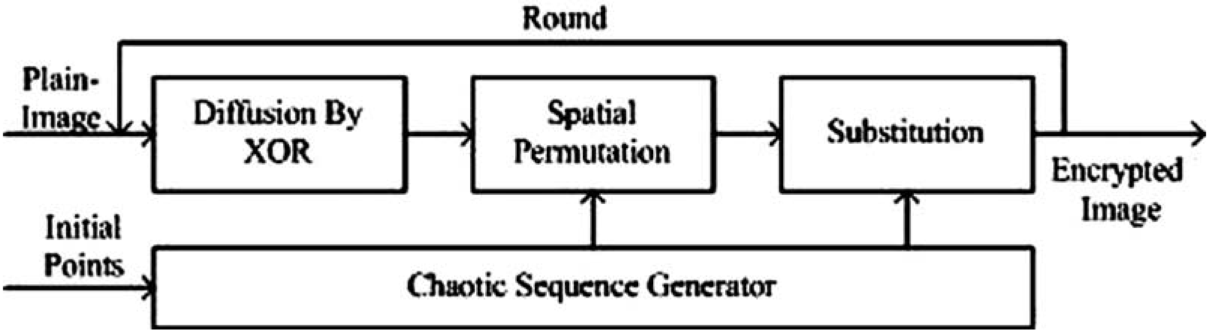

Figure 2.4: diagram of the image secret writing [24].

In this paper authors square measure stress on image encryption’s appropriate methodology to guard image knowledge. Image and text knowledge has their distinctive options. The out their encoding algorithms square measure sensible for text knowledge. They will not be appropriate for transmission knowledge. In truth the pixels of natural pictures square measure extremely related to their neighbour pixels. As a result of this sturdy correlation any constituent is much expected from the values of its neighbours. During this article, we have a tendency to propose a brand new location transformation based mostly encoding technique. We have a tendency to distribute the constitutional values of totally different location victimization affine rework technique with four 8-bit keys. The remodelled image then divided into two x two pixel blocks and every block is encrypted victimization XOR operation by four 8-bit keys. The entire key size utilized in our algorithmic rule is a sixty four bit that proves to be sturdy enough. The experimental results tried that when the engine rework the correlation between constituent values was considerably shrivelled [25].

According to Sandeep Bhowmik, Sriyankar Acharyya, Evidently, data security may be a circular function qua non within the "modern life, with its unwell rush, its divided aims, Its heads overtaxed, it's unsteady hearts". To shield our knowledge against unauthorized access, from the time out of mind the primary alternative has invariably been to use cryptography. With rising within the arena of transmission technology, since digital image has become a vital medium of communication, in depth analysis continues to be a dynamic method during this field. We tend to even have targeted image encoding during this work. The effectiveness of the protection through encoding depends on the algorithmic program applied and in addition as on the standard of the 'key' used. If a 'key' is badly designed or haphazardly chosen, clearly the protection fails to supply correct security and improper access may be gained on the secured data. The primary algorithmic program in cryptographic system style is that the algorithmic program to come up with 'key'. It specifies the way within which the 'key' is to be chosen. This work focuses on a completely new approach towards the 'key' generation of encoding algorithms. Here, the Genetic algorithmic program (GA), a vital methodology of computer science has been applied to come up with encoding key that plays an important role in any sort of encoding. In our work, a hybridized technique known as BlowGA is additionally projected that may be a combination of Blowfish and GA. The blowfish algorithmic program may be a typical methodology of encoding. Our experimental observations show that the newly-proposed hybridized methodology BlowGA outperforms each GA and Blowfish algorithmic program [26].

III. CONCLUSION:

Following are the conclusions:

1. Cryptography algorithm for image is not so easy. RES, AES, DES are not suitable for colour images, which are 2D arrays of data.

2. There is a new version of Image Encryption Algorithm (IEA) is required to developed, which need less computation than the old version and accomplish the same encryption results.

3. Some algorithm can accomplish an acceptable quality of service and need an appropriate different security level of the image data.

4. Chaotic maps, Baker and Cat map, standard map, tent map and logistic map techniques are used for multimedia cryptography (like image, video and audio data).

5. Some cryptography algorithm model based on the orthogonal transforms for images. Symmetric key cryptography use malakooti Raeisi (M-R) transformation algorithm for key generation of HT, MT and DCT.

6. A lossless digital encryption system for images used orthogonal transforms matrix and XOR operations are used for the improved cryptography algorithm.

REFERENCES:

[1] G.R. Blakley, Twenty years of cryptography in the open literature, Security and Privacy 1999, Proceedings of the IEEE Symposium, 9-12 May 1999.

[2] W. -K. Chen, Scott Sutherland, "An Introduction of Cryptography",MSTP MATH WORKSHOP, 2005.

[3] Forouzan - Behrouz .A "Cryptography And Network Security", McGraw Hill. 2008.

[4] William Stallings, "Cryptography and Network Security Principles and Practices", Prentice Hall. 2006.

[5] Khan UM, Kh M. Classical and chaotic encryption techniques for the security of satellite images. In: IEEE international symposium on biometrics and security technologies (ISBAST 2008), vol. 5, no. 23–24; 2008. p. 1–6.

[6] Matthews R. On the derivation of a chaotic encryption algorithm. Cryptologia 1989;13(1):29–42.

[7] Amigó JM, Szczepanski KL. Theory and practice of chaotic cryptography. Phys Lett A 2007;366(3):211–6.

[8] Li S, Alvarez G, Li Z, Halang WA. "Analog chaos-based secure communications and cryptanalysis: a brief survey", Proceedings of 3rd international IEEE scientific c

[9] Zhang L, Liao X, Wang X. An image encryption approach based on chaotic maps. Chaos, Solitons & Fractals 2005;24(3):759–65.

[10] Pareek N, Patidar V, Sud K. Discrete chaotic cryptography using external key. Phys Lett A 2003; 309:75–82.

[11] Pareek N, Patidar V, Sud K. Image encryption using chaotic logistic map. Image Vis Comput 2006; 24(9):926–34.

[12] Kwok HS, Tang Wallace KS. A fast image encryption system based on chaotic maps with finite precision representation. Chaos, Solitons & Fractals 2007;32(4):1518–29.

[13] Behnia S, Akhshani A, Mahmodi H, Akhavan A. A novel algorithm for image encryption based on mixture of chaotic maps. Chaos, Solitons & Fractals 2008;35(2):408–19.

[14] Fridrich J. Symmetric ciphers based on two-dimensional chaotic maps. Int J Bifurc Chaos 1998;8(6):1259–84.

[15] Mao Y, Chen G, Lian S. A novel fast image encryption scheme based on 3d chaotic baker maps. Int J Bifurcat Chaos 2004;14(10):3613–24.

[16] Chen G, Mao Y, Chui CK. A symmetric image encryption scheme based on 3D chaotic cat maps. Chaos, Solitons & Fractals 2004;21(3):749–61.

[17] Guan ZH, Huang FJ, Guan WJ. Chaos-based image encryption algorithm. Phys. Lett. A 2005;346:153–7.

[18] Lian S, Sun J, Wang Z. A block cipher based on a suitable use of chaotic standard map. Chaos Solitons and Fractals 2005;26:117–29.

[19] Li S, Chen G, Zheng X. Chaos-based encryption for digital images and videos. In: Multimedia security handbook. LLC, Boca Raton, FL, USA: CRC Press; 2004. p. 133–67 [chapter 4].

[20] Mao Y, Chen G. Chaos-based image encryption. In: Bayro-Corrochano E, editor. Handbook of computational geometry for pattern recognition, computer vision, neural computing and robotics. Springer; 2003.

[21] Amir- Masud Eftekhari-Moghadam Sahar Mazloom "Color Image Cryptosystem using Chaotic Maps", IEEE; Qazvin Islamic Azad University Qazvin, Iran; 2011; 978-1-4244-9915-1/1.

[22] Bibhudendra Acharya, Sambit Kumar Shukla, Saroj Kumar Panigrahy, Sarat Kumar Patraand Ganapati Panda "H-S-X Cryptosystem and Its Application to Image Encryption"IEEE,International Conference on Advances in Computing, Control, and Telecommunication Technologies, 2009, 978-0-7695-3915-7/09.

[23] N.K. Pareek, Vinod Patidar, K.K. Sud "Image encryption using chaotic logistic map" , Received 10 August 2004 Image and Vision Computing 24 (2006) 926–934

[24] Linhua Zhang ,Xiaofeng Liao, Xuebing Wang, "An image encryption approach based on chaotic maps" Department of Computer Science and Engineering, Chongqing University, Chongqing, China,2005, 759–765 www.elsevier.com/locate/chaos.

[25] Amitava Nag, Jyoti Prakash Singh, Srabani Khan, Saswati Ghosh, Sushanta Biswas, D. Sarkar, Partha Pratim Sarkar , "Image Encryption Using Affine Transform and XOR Operation", Dept. Of Information Technology, Academy of Technology Bandel, India, Proceedings of 2011 International Conference on Signal Processing, Communication, Computing and Networking Technologies (ICSCCN 2011).

[26] Sandeep Bhowmik, Sriyankar Acharyya, "Image Cryptography: The Genetic Algorithm Approach" Department of Computer Science & Engineering, Hooghly Engineering & Technology College Hooghly, India 978-1-4244-8728-8/11/$26.00 ©2011 IEEE