International Journal of Recent Trends in Engineering & Research
ISSN (ONLINE) : 2455 – 1457
IMPACT FACTOR : 4.101

ENERGETIC DATA SECURITY SCHEME VIA IMAGE AS CRYPTO KEY NATURE

E. PRAGNAVI[1], G.KISHORE KUMAR[2]
[1,2]Assistant Professor,Department of CSE, UCE (A) OU, Hyderabad, Telangana, India.

Objective: - The main objective of this system is to propose a methodology which is more efficient and secure for maintaining the data or information in safer manner with advanced Cryptographic Algorithms. In this methodology, a new scheme is introduced to secure the data, which is called "Image as a Key" method. With the help of this method we can use the Image as a key for securing or encrypting the data, in other words the given image is act as a Cryptographic Key for the data need to be secure.

I. INTRODUCTION

Now-a-days information security and its maintenance is the major concentration for all Information technology, Government and Non-Government Organizations. The main motto of this system is to preserve the data integrity and data security with more advanced manner and resolve the issues in present scenarios of data security. Information management plays a vital role in more business and organizational scenarios such as Banking, Stock Market, Educational Institutions, Shopping Sectors and many more places. So that lots of new mechanisms are derived to produce the energetic or efficient solution for this case, and most of the researchers invent lots of algorithms in past to produce certain level of solutions using cryptographic methods such as Block Image Encryption Algorithm, Mirror-Like Image Encryption Algorithm, Chaotic-Like Image Encryption Algorithm, Image Encryption using Digital Signatures and so on.

All these algorithms produces better results in various stages of data security but the level of data safety is not yet to be guaranteed at any case. For these issues a new methodology is required to manipulate all the security oriented solutions and provide the best solutions to user to make their data more safe compare to all existing analysis. A new "Image as a Key" methodology is introduced to resolve these problems and in this proposed scheme considers image as a cryptographic key which is used for securing the data with more advanced manner, that is the image we are taken as an input is encrypted and it serve to the data for making that data to be encrypted and that input image is considered to be a key to the data to decrypt.

The main idea behind this apprpach is making a new definition for information security with the help of digital images and involves that key to act as a major component in information security scenario as well as maintain the data in more secured and efficient manner. With this technique the proposed approach can prove its efficiency and provide the best result or level of data security and integrity compare to all the other approaches in past.

II. AUTHENTICITY AND DATA INTEGRITY

Authenticity concerns the honesty of starting points, traits, responsibilities, earnestness, commitment, and expectations. Data Integrity is the term which reveals the realistic and actual propositions of data in fine manner, simply illustrates the integrity level of data which is actually be like on the creation time. The data can be tested with two norms to prove its security level such as Authentic and Integretic. Authentic is the term reveals the fact that the data is properly opened or accessed by the respective person and the term integritic refers to the data to be properly closed by the person with the same level of content and concepts which is presented in beginning [at the time start accessing the document/data/information].

2.1 Data Security – A New Way

Data security is not simply to give validness and honesty to the information, however there is likewise a need to look for personality, privileges of utilization and root of data, which may require some level of process re-building. With the quick development of advanced information trade, security data turns out to be much vital in information stockpiling and transmission.

Cryptography is fundamentally securing the information amid the correspondence between various frameworks. To give the security of information amid correspondence in cryptography we together require the algorithm as well as Key.

The classification and honesty of the information amid correspondence depends halfway on calculation and incompletely on key. Because of human memorizability the measure of key in cryptography is restricted. The key size is also complex to remember at all the time of extractions of actual data. And the key based data cryptography is a classical technique, which provides the data security by means of either public key or by means of private key. This kind of data security is secured as well but the complexities and issues according with these are really complex as well as that all are described in above descriptions. So that a new methodology is required to provide the data security in more intelligent manner with full of trustworthiness and safer manner. The concept of Image as a Key is introduced on this scenario to prove the intelligence and efficiency of data security and trustworthiness.

Cryptography is about correspondence within the sight of a foe. It comprises of numerous issues like encryption, verification, and key dissemination. The field of current cryptography gives a hypothetical establishment in light of which one can comprehend what precisely these issues are, the manner by which to assess conventions that support to understand them and how to construct conventions in whose security one can have certainty. Progressed advanced innovations have made sight and sound information generally accessible. As of late, sight and sound applications end up noticeably regular practically speaking and along these lines security of mixed media information has turned out to be principle concern. As of late, data can be safely transmitted by implanting the data in images and utilizing water stamping methods.

The idea is to focus on the key which is utilized as a part of various calculations. Proposition is to utilize image for era of an open key which is utilized for encryption of information in encryption calculations. The major taught behind this concept is an image which is utilized as a key ought to ready to be encoded/ unscrambled. This scrambled image can be utilized as a key for encryption of information.

2.2 Image as a Key

The more intelligent Image based Data Security scheme is introduced with the help of Image as a Key methodology. With this method user can secure the data or information in fine manner. In this

system user have to select an input image as well as the user have to provide the corresponding data to be encrypted/secured. This proposed Image as a Key approach encrypts the input image and set that a Key to the data to be encrypted, after processing the image it comes for data to encrypt according with the image key specified earlier. For all the entire data is encrypted in safer manner with the help of this Image as a Key methodology. The concept is clearly explained by means of the following system design.

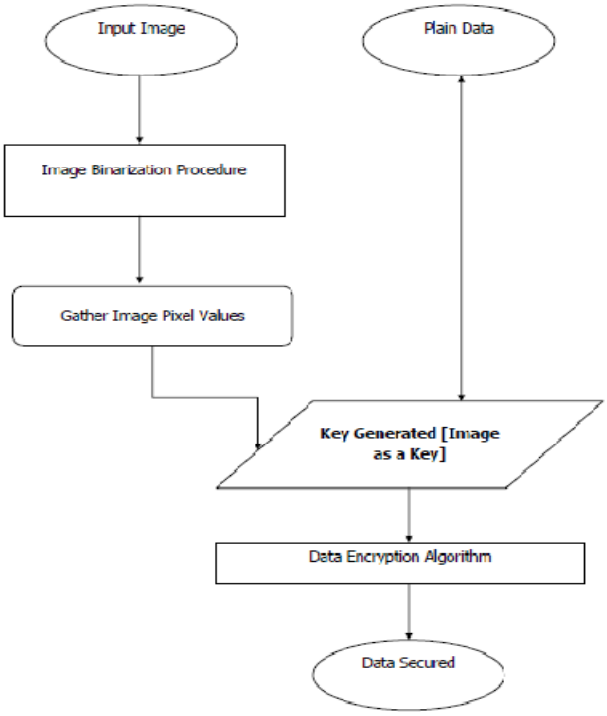

Fig 1: Image as a Key methodology

The above figure of system design starts with the flow of Input Image as well as the Plain Text which is to be secured. The input image is applied to the binarization procedures and the preprocessing stages such as gray scale conversion and pixel modulations to get the RGB extractions of pixel values. Once this procedure is completed some random values are gathered from the pixel values as well as the plain text is to be encrypted with the help of those randomly selected pixel values from the input image. The algorithm called Data Encryptions Standard [DES] is applied to make the encryption process more safely and provides the results more better compare to the existing scenarios.

III. IMAGE ENCRYPTION PRINCIPLES

The digital signature and watermarking techniques are utilized for image validation where Digital mark encodes the mark in a record isolate from the first image.The advanced mark made for the first image and apply watermark. images are resized before transmission in the system. After digital mark and water denoting a image, apply the encryption and decoding procedure to a image for the verification. The encryption is utilized to safely transmit information in open systems for the encryption of a image utilizing open key and unscramble that image utilizing private key.

Advanced mark is a kind of Cryptography comparable as the written by hand signature on a paper and it having the digital authentication utilizing this checks the identity. Watermarking is a sub-train of data covering up where the data is embedded into an advanced flag in a way that is hard to

expel. It's giving copyright assurance to scholarly technique that is in digital format. The cryptography is giving better components to data security."Digital Signature and Digital Watermark Scheme for Image Authentication consolidated and connected to a host image. The first images are having the water check and apply the digital signature on it before the transmission in the internet. An Algorithm of Encryption and Decryption of Images Using Chaotic Mapping frames a critical field of data security where turbulent mapping connected on plain-image.

There are plans which utilize connection examination to recognize implanted mark to validate message. Another plan utilizes Gauss-Jordan strategy to get the mark from the watermarked image to confirm proprietorship which is verified with result and utilization of the method to avert phony and modification in e-check report. Because of the expanding utilization of images in mechanical process, it is basic to shield the secret image information from unapproved get to. The Advanced Encryption Standard [AES],has been broke down and by include a key stream generator [A5/1, W7] to AES to guarantee enhancing the encryption execution; predominantly for images described by diminished entropy.

Extended Visual Cryptography is a kind of cryptography which encodes various images in the way that when the images on transparencies are stacked together, the concealed message shows up without a hint of unique images. The unscrambling is done specifically by the human visual framework with no uncommon cryptographic computations. While the past inquires about essentially handle just double images, this presents a framework which takes three images as information and creates two images which relate to two of the three information images where the third image is remade by printing the two yield images onto transparencies and stacking them together as well as Extended visual cryptography plot appropriate for regular images. Some new image encryption plans have been proposed, where the encryption procedure includes a change operation and a XOR like change of the rearranged pixels, which are controlled by clamorous frameworks.

IV. LITERATURE STUDY

In this summary, we describe lots of image encryption techniques and its procedures clearly.

In the year of 1997, the author Jiri Fridrich proposed a new algorithm called Block Image Encryption Algorithm, which illustrates an encryption algorithm that adapted certain invertible chaotic two-dimensional maps to create new symmetric block encryption schemes. This scheme is especially useful for encryption of large amount of data, such as digital images.

In the year of 1999, the authors Jiun-In Guo and Jui-Cheng Yen illustrate a new algorithm called Mirror-Like Image Encryption Algorithm and Its VLSI Architecture, which presents a technique based on a binary sequence generated from a chaotic system, an image is scrambled according to the algorithm. This algorithm possesses low computational complexity, high security and no distortion.

In the year of 2000, the authors Jui-Cheng Yen and Jim-In Guo demonstrate into their algorithm called Chaotic-Like Image Encryption Algorithm and Its VLSI Architecture, which is an image encryption/decryption algorithm and its VLSI architecture proposed. According to a chaotic binary sequence, the gray level of each pixel is XORed or XNORed bitby-bit to one of the two predetermined keys.

In the year of 2001, the author Shoby described into her new algorithm called Chaotic Image Encryption Algorithm, in which it uses Lorenz equation for encryption, creating secure databases; secure

Email,implemented in FPGA for real time images. In this paper the chaotic algorithm is used for encrypting text and images. In [5] attacks on chaotic algorithm have also been discussed.

In the year of 2003, the authors Aloka Sinha and Kehar Singh proposed an algorithm called Image Encryption using Digital Signatures, in which it have proposed a new technique to encrypt an image for secure image transmission. The digital signature of the original image is added to the encoded version of the original image. Image encoding is done by using an appropriate error control code, such as a Bose-Chaudhuri Hochquenghem [BCH] code. At the receiver end, after the decryption of the image, the digital signature has been used to verify the authenticity of the image.

V. CHINESE REMAINDER THEOREM

In the greater part of the real-world applications images are utilized as a part of request to secure data exchanging on the web or any other medium. Cryptography with images is the rising idea in the specialized world. To meet this test number of strategies were proposed. All things considered we focused on the best way to fortify the key of encryption calculations utilizing images with Chinese Remainder Theorem [CRT]. Out approach is to create a variable length key from image considering image highlights like shading with Chinese Remainder Theorem which is utilized as a part of encryption and decoding process. This proposition can frame solid and productive technique to reinforce the key of encryption calculation.

The key which is utilized as a part of encryption calculations is to be produced utilizing images considering one of the image highlights like shading, edge, edge and so on. In this paper we consider one of the highlights i.e shades of image in the era of key and use of Chinese Remainder Theorem to reinforce the security of key. In this, the information is taken as RGB image which is resized to particular size. Later this resized RGB image is utilized as a part of getting red shaded image utilizing one of the techniques in MatLab. At that point a grid is acquired considering the red image pixel esteems. From this network, haphazardly three numbers are chosen and these three numbers are checked for generally prime. On the off chance that the condition is met i.e numbers are generally prime, at that point these numbers progress toward becoming contribution to Chinese Remainder Hypothesis. At that point an arrangement of qualities are acquired as results on utilization of CRT of which one esteem is haphazardly chosen for key of variable length is clarified before. This arbitrarily chose variable length key is utilized as a part of symmetric encryption calculations for online secure data exchange.

Theorem: CRT

Step-1: Get the Image and start processing such as image re-sizing as well as Convert it into red-colored nature.

Step-2: From the red-colored image, a moderate framework of I[m x n] is acquired considering the pixel esteems of red hued image where m, n characterizes the measure of the framework. From this I[m x n] framework, expel the zero esteems what's more, acquire the last grid Fv.

$$Fv=removezeroes[I[m\ x\ n]]$$

Step-3: From conclusive framework Fv, select m number of non-zero values in view of the symmetric calculation utilized.

$$M=random[x,Fv]$$

where x is a variable characterizing number of qualities to be chosen from Fv.

Step-4: The M chose numbers are confirmed for generally prime.

Step-5: The above chose relative prime numbers are utilized as contributions to CRT calculation and the yield of CRT is P number of qualities which frames a hotspot for irregular choice of variable length key. This variable length key is utilized as a part of data encryption and unscrambling handle.

Step-6: From the above strides, from a solitary chose image P number of qualities created which are framing hotspots for keys of symmetric encryption calculations. The aggregate number of P esteems increments as the M esteems builds which are utilized as keys in symmetric encryption calculations.

One Time Password [OTP]

In this summary Image Based Password System [IBPS] is highly concentrated and it produces the One Time Password called OTP, which provides the high security one time system generated random numbers for characteristic pulling out of images and provide that to users to encrypt the data with the help of this OTP. IBPS can resolve and address the security issues of above plans. Even, the security level of IBPS is high and it is extremely hard to break such passwords utilizing typical assaults.

The following figure clearly explains the principle of Image Based Password System and its system analysis procedures in clear manner as well as the functionality of One Time Password [OTP].

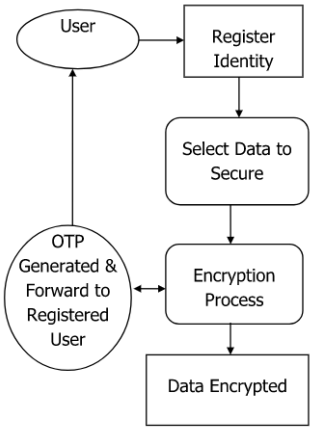

Fig 2: Image Based Password System

VI. EXPERIMENTAL RESULTS

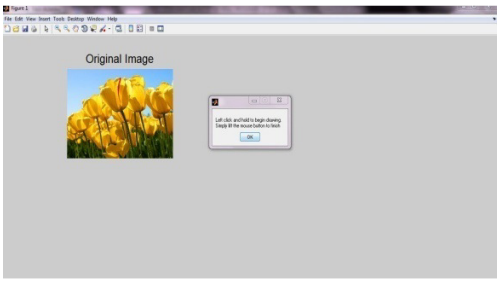

Fig.3. Input Image

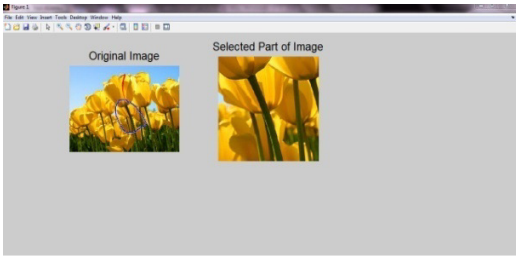

Fig.4 Selected RGB Portion of Input Image

Final Matrix Fv

CroppedImage(:,:, 1) =

Columns 1 through 16

235	250	204	206	228	206	198	171	165	188	196	217	226	179	185	189
209	208	194	197	192	192	199	172	161	187	201	226	232	185	191	195
194	195	191	196	191	188	199	174	167	184	208	231	236	186	204	208
194	194	193	197	192	194	202	169	164	186	216	244	234	191	206	211
188	188	190	194	187	189	199	162	163	189	217	250	231	201	213	211
184	184	186	191	189	186	192	164	168	194	223	249	232	207	224	213
183	190	191	189	189	191	188	162	170	202	240	255	227	210	225	218
189	188	194	195	189	191	184	164	178	207	249	255	217	218	225	223
185	192	200	200	191	200	188	173	198	235	255	251	216	226	232	228
190	207	210	195	197	209	199	206	230	251	255	246	220	229	237	236
243	253	250	234	235	247	227	239	255	255	255	242	226	239	239	243

Fig.5 Matrix from Selected RGB Portion of Input Image

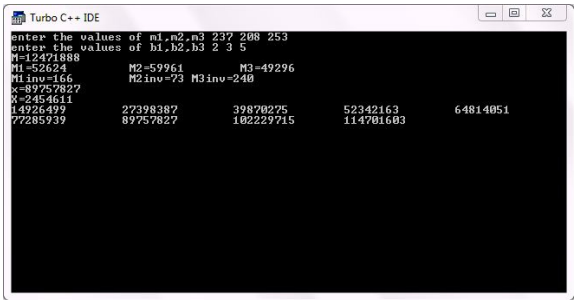

Fig.6 CRT Output for the Given Inputs

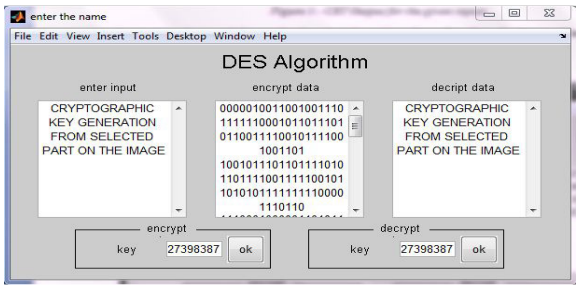

Fig.7 DES Algorithm Implementation

REFERENCES

Books:-

1. Cryptography and Network Security by William Stallings
2. Network Security Essential by William Stallings

Papers:-

I. Jiri Fridrich, "Image Encryption Based on Chaotic Maps", Proceeding of IEEE Conference On Systems, Man, and Cybernetics, pp. 1105-1110, 1997.

II. Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China in 1999.

III. Jui-Cheng Yen, and Jiun-In Guo, "A New Chaotic Key-Based Design for Image Encryption and Decryption", IEEE International Symposium on ISCAS 2000, Geneva, pp. IV-49-IV-52, May. 2000.

IV. M.I.Sobhy, and A.R.Shehata, "Chaotic Algorithms for Data Encryption", IEEE Proceeding of ICASSP 2001, Vol 2, pp.997-1000, May. 2001.

V. M.I.Sobhy, and A.R.Shehata, "Methods of Attacking Chaotic Encryption and Countermeasures", IEEE Proceeding of ICASSP 2001, Vol 2, pp. 1001-1004, May. 2001.

VI. Aloha Sinha, Kehar Singh, "A technique for image encryption using digital signature", Optics Communications, ARTICLE IN PRESS, 2003, 1-6, ww.elsevier.com/locate/optcom

VII. Chang-Mok Shin, Dong-Hoan Seo, Kyu-Bo Chol, Ha-Wmn Lee, and SmJmng Kim, " Multilevel Image Encryption by Binary Phase XOR Operations ", IEEE Proceeding in the year 2003.

VIII. Fethi Belkhouche and Uvais Qidwai ,"Binary image encoding using 1D chaotic maps", IEEE Proceeding in the year 2003.

IX. Wang Ying, Zheng DeLing, Ju Lei, et al., "The Spatial-Domain Encryption of Digital Images Based on High-Dimension Chaotic System", Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172-1176,December. 2004

X. M.-R. Zhang, G.-C. Shao and K.-C. Yi, " T-matrix and its applications in image processing", IEEE Electronics Letters 9th December 2004 Vol. 40 No. 25

XI. Shaojiang Deng, Linhua Zhang, and Di Xiao, "Image Encryption Scheme Based on Chaotic Neural System", J. Wang, X.Liao, and Z. Yi (Eds.): ISNN 2005, LNCS 3497, pp. 868-872, 2005.

XII. Huang-Pei Xiao Guo-Ji Zhang "An Image Encryption Scheme Based On Chaotic Systems", IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.

XIII. Guosheng Gu ,Guoqiang Han "An Enhanced Chaos Based Image Encryption Algorithm", IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06) in 2006.

XIV. H. Cheng and X. Li, "Partial Encryption of Compressed Images and Video," IEEE Transactions on Signal Processing,48(8), 2000, pp. 2439-2451.

XV. M. Van Droogenbroeck and R. Benedett, "Techniques for a Selective Encryption of Uncompressed and Compressed Images," Proceedings of Advanced Concepts for Intelligent Vision Systems (ACIVS) 2002, Ghent,Belgium, September 9-11, 2002.

XVI. M. Podesser, H.-P. Schmidt and A. Uhl, "Selective Bitplane Encryption for Secure Transmission of Image Data in Mobile Environments," 5th Nordic Signal Processing Symposium, on board Hurtigruten, Norway, October 4-7, 2002.

XVII. IEEE Transactions on Circuits and Systems for Video Technology: Special Issue on Authentication, Copyright Protection, and Information Hiding, Vol. 13, No. 8, August 2003.

XVIII. X. Liu and A.M. Eskicioglu "Selective Encryption of Multimedia Content in Distribution Networks: Challenges and New Directions," IASTED International Conference on Communications, Internet and Information Technolog (CIIT2003), Scottsdale, AZ, November 17-19,2003.