IFERP
connecting engineers... developing research

ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 3, Issue 11, November 2016

Intelligent Key Based Data Security Scheme with Modified Key Image Resemblance

[1] T.Augustine, [2] P.Vasudeva Reddy, [3] P.V.G.D. Prasad Reddy
[1] Research Scholar, [2][3] Professor
[1][2] Department of Engg. Mathematics, Andhra University, Visakhapatnam, AP, India.
[3] Professor, Department of CS&SE, Andhra University, Visakhapatnam, AP, India

***Abstract*— Crypto Systems are still the most believable security consideration till today. There have been consistent efforts by the researchers and analyzers over the decades to produce several kinds of security measurements and enhancements over cryptography to improve the data security features. However in spite of all the efforts, providing high security of data over the network still remained a challenging problem. A new idea to implement the security terminology that provides confidence to the users to preserve the data in any place with maximum level of security is always welcome. In this paper a new methodology for data encryption is proposed, which is called Modified Key Image Resemblance [M-KIR]. Through this M-KIR approach, the way of encryption is done with high secured feature called Image as Key. This means the digital-images are used as the keys to encrypt the data. By applying this logic, users can secure the data with M-KIR protection with high level of security. Since the digital image is being used as a key, it is highly difficult for the attackers and hackers to attain the encrypted data. Lot of experiments were carried out at the experimental phase of this project and the proposed Modified Key Image Resemblance Scheme has been proved to guarantee robust and highly-favorable data encryption standard and powerful crypto principles in resulting strategies..**

Keywords— Crypto Systems, Encryption-Decryption Methodologies, Modified Key Image Resemblance, MKIR, Data Security and Integrity.

I. INTRODUCTION

In an information security domain, secrecy and privacy are the most important concerns to deal with for any transactions over the network. It is a known fact that the main objective of data security and privacy is converting the original data into non-readable format by using crypto-terminologies. By means of unauthenticated accessing and misusing natures, lots of private records are being stolen by the hackers and attackers. It is noted that this causes a major issue in the mining and multimedia data processing unit. For avoiding this kind of data threats, lots and lots of methodologies are being designed by the developers and implemented for many decades of research in the area of cryptography. However, all these research works are strucked up at certain stage and paved a way to attack-injection precedence because of poor and insufficient intelligence in processing and evaluation.

In the literature, many approaches are found, where lots of key sharing methodologies are available such as: Symmetric Key Crypto systems, which share the public and private keys between sender and receiver to make secure the data such as: AES, DES and so on. Similarly, in case of asymmetric crypto systems uses key sharing principles in different way such as sharing the public key between both entities but private keys in single entity and which is securable and possible to known only to the recipient end, so that the data can easily be decrypted into the receiver end, the available asymmetric key crypto schemes are Rivert-Shamir and Adelman Algorithm, Hellman Algorithm and so on. The realism and processing characteristics of all the defined algorithms are trying to prove one possible constraint called security but the way of approaching the data cryptography is different in case of precedence.

The key length of each algorithm differs from one and another, but all are depending on the algorithm characteristic and features, which are purely based on the norms followed by the numeric constraint produced from the algorithm principle and processing nature. The strength of the algorithm depends on various characteristics such as key-size, iteration norms, text-complexity and size-of-data. These logics are different and complex in case of processing, but the attackers use the common breakable logic to process the keys, because all these existing logics use the common alpha-numeric key logics, so such keys are easily breakable and guessable to recover. This gives the motivation for a new system to be designed and implemented to avoid these kinds of attacks and possible guesses to break the data attacking and integrity affections.

II. SOME OF THE EXISTING ALGORITHMS IN THE LITERATURE

In the year of 2003 [1], the authors "Tetsuji Takada and Hideki Koike2, Awase-E" proposed a paper titled "Image-based Authentication for Mobile Phones using User's Favorite Images", in that they described such as: there is an exchange off amongst security and convenience in client validation for cell phones. Since such gadgets have a poor information interfaces, 4-digit number passwords are generally utilized at exhibit. In this manner, a more secure and easy to understand validation is required. This paper proposes a novel verification strategy called "Awase-E". The framework utilizes picture passwords. It, additionally, incorporates picture enlistment and warning interfaces. Picture enrollment empowers clients to utilize their most loved picture rather than a content secret key. Notice gives clients a trigger to make a move against a danger when it happens. Awase-E is actualized so it has a higher ease of use notwithstanding when it is utilized through a cell phone. Even earlier to this for Image Cryptosystems, New Encryption Algorithm was proposed by Chin-Chen Chang, Min-Shian Hwang, and TungShou Chen [6]. During encryption, the image is compressed using a popular image compression technique named vector quantization concept and encrypted. This proposal achieves high security and low computations during encryption and decryption of images.

In the year of 2010[2], the authors "Patra, Jagdish Chandra; Karthik, A, Bornand, Cedric" proposed a paper titled "A novel CRT-based watermarking technique for authentication of multimedia contents", in that they described such as: Advanced watermarking methods have been proposed as an answer for the issue of copyright assurance of media information. In this paper, we propose a novel Chinese leftover portion hypothesis (CRT)- based strategy for computerized watermarking. The utilization of CRT for this reason gives extra security along protection from some well-known assaults. We have demonstrated that this system is very strong to expansion of the commotion. We have contrasted execution of the proposed method and as of late revealed two particular esteem disintegration (SVD)- based watermarking systems and demonstrated its unrivaled execution regarding altering evaluation work (TAF), computational effectiveness and pinnacle flag to commotion proportion (PSNR). For instance, the installing time of the proposed CRT-based plan is 6 and 3 times quicker than the SVD-based Schemes 1 and 2, separately. This procedure can likewise be connected to report, sound and video substance. A new biometric authentication system using finger-knuckle-print (FKP) imaging has been proposed by Lin Zhang, Lei Zhang, David Zhang, Hailong Zhu [10]. In order to capture the FKP images a specific device is constructed which is stored in an image database.

Again in the same year of 2010, the authors "Seyed Mohammad Seyedzade, Reza Ebrahimi Atani, Rasht" [7] proposed a paper titled "A novel image encryption algorithm based on hash function", in that they described such as: a novel calculation is intended for picture encryption in light of SHA-512 is proposed. The primary thought of the calculation is to utilize one portion of picture information for encryption of the other portion of the picture equally. Particular attributes of the calculation are high security, high affectability and rapid that can be connected for encryption of dim level and shading pictures. The calculation comprises of two primary segments: The first does preprocessing operation to rearrange one portion of picture. The second uses hash capacity to create an arbitrary number cover. The veil is then XORed with the other piece of the picture which will be encoded. The point of this work is to build the picture entropy. Both security and execution parts of the proposed calculation are dissected and tasteful outcomes are accomplished in different rounds. On the other side another image encryption method using Differential Evolution Approach was proposed by Ibrahim S I Abuhaiba and Maaly A S Hassan [8]. In this, 2D keyed Discrete Fourier transform is applied on the image which is to be encrypted and then the concepts of linear feedback shift register index generator, keyed mutations and simple diffusion mechanisms are implemented in the encryption process

In the year of 2013, the authors "QuisAphetsi Kester" [5] proposed a paper titled "Image Encryption based on the RGB PIXEL Transposition and Shuffling", in that they described such as: Protection is one of the key issues data Security addresses. Through encryption one can keep an outsider from understanding crude information amid flag transmission. The encryption strategies for upgrading the security of advanced substance has increased high importance in the present period of rupture of security and abuse of the secret data captured and abused by the unapproved parties. This paper embarks to add to the general assortment of learning in the region of cryptography application and by building up a figure calculation for picture encryption of m*n measure by rearranging the RGB pixel esteems. The calculation at last makes it feasible for encryption and decoding of the pictures in light of the RGB pixel. The calculation was executed utilizing MATLAB.

In the year of 2015, the authors "Ashraf Odeh, Aymen Abu-Errub, Mohammed Awad [3] proposed a paper titled "Symmetric Key Generation Method using Digital Image", in that they described such as: another key age calculation is composed in view of utilizing a double picture. The proposed calculation changes over 16×16 paired exhibit speaking to the advanced picture into 4×4 cluster, at that point it changes over the new created exhibit into 4×4 decimal cluster. The decimal cluster and the left slanting of the first exhibit are then used to create the general population key that is utilized to scramble the information to be sent for the beneficiary. The proposed calculation is likewise utilized as a part of the collector side to create the private key used to decode the encoded information.

In the year of 2016 [4], the authors "Abdulrahman Dira Khalaf" [4] proposed a paper titled "Fast Image Encryption based on Random Image Key", in that they described such as: Web assumes an imperative part in coursing a gigantic measure of sight and sound. A case of this mixed media is the picture. To send a picture over the system covertly, the sender tries to discover encryption calculation to shroud picture data. This paper goes for planning a proficient encryption calculation for shading picture utilizing arbitrary picture key produced with least time execution for encryption and decoding operations. XOR operation is utilized here to make more dissemination of the encoded picture to keep up a larger amount of security upon transference than it is with the first picture. An authentication method for a moving image was proposed in [11] by Ren Fujii, Yasunari Yoshitomi, Taro Asada, Masayoshi Tabuse. They proposed two methods; one is an authentication method for a moving image by using discrete wavelet transform and the other is a method for selecting several frames in the moving image. This method avoids insertion of additional information into the actual moving image and encourages using the extracted features of the image for authentication

In spite of various contributions that are found in the literature, it may be concluded that despite decades of research in the area of cryptography, providing complete data/information security and integrity remained as a problem. Although many researchers, over the years have suggested various approaches to resolve this problem, it still remained incomplete, challenging and seeking new contributions. Thus it has become very important for researchers experimenting with new methodologies in providing high security. This context gave motivation to the present research investigation, to study, improve and examine the possibility of implementing the Intelligent Key Based Data Security Scheme with Modified Key Image Resemblance

III. PROPOSED DATA SECURITY LOGICS

In this proposed approach of data security Modified Key Image Resemblance [MKIR] logic is used, which is a 256-bit encryption scheme and also performs the cryptography of data in same precedence as per the existing algorithms, but the difference is this algorithm uses the crypto logic that is instead of using the crypto key, this proposed system uses digital images as keys to the data which is going to be secured. The users are required to provide the input in two stages, first is data and next is digital image. The processing starts with the extraction of image features such as pixels ranges, RGB combinations and image size. Based on these features, this algorithm generates the key in different size nature, which is not easy to be guessed and cannot be hacked simply by using random guesses.

In this new approach of data security, the principle of obtaining the security is different, because a 256-bit data encryption standard is applied with different set of key management laws that are derived from the digital image features. Even on the receivers end, the recipient is required to pass the input at two stages, at the first stage, the recipient has to provide the encrypted data, which is to be decrypted and then the digital image to decrypt the data. The experimental results have shown that the proposed method performs better in providing safer and secure data encryption in real-time usages.

Modified Key Image Resemblance [M-KIR] Scheme

A new methodology of data security scheme is proposed to process the data with high level of prevention and provides guarantee to the users to share the data efficiently between one and another without any fear of data being stolen.

The proposed system introduces a new data processing and encryption scheme, called Modified Key Image Resemblance [M-KIR] algorithm, which process the data with ultimate preference of data security with the help of digital images. Initially the input data is provided for processing and the next stage is to resemble the input image to further enhancement of security features. The data is processed with image features, such as extracting the digital image feature such as color correlation, size of image, pixel ranges and other related features.

The Key Generation Technique in the proposed methodology is as follows: First of all a set of RGB images are taken from which one image is selected and resized. This resized image will be shown to the end user where the end user would select certain number of points on the resized image. Now the pixel values of the selected point of the image are displayed as a result. Then based on the predefined number, those number of values will be selected randomly from the displayed selected point pixel values. After this, these randomly picked values are verified for relative prime condition. If the numbers are relatively prime then apply them as input to Chinese Reminder Theorem. For secure key, to make key disclosure, more complex and to make key stronger Chinese Remainder Theorem (CRT) is used [12]. A set of values as an output of Chinese Reminder Theorem forms a source for random selection of variable length key. A variable length key is selected accordingly to the algorithm in data encryption and decryption process.

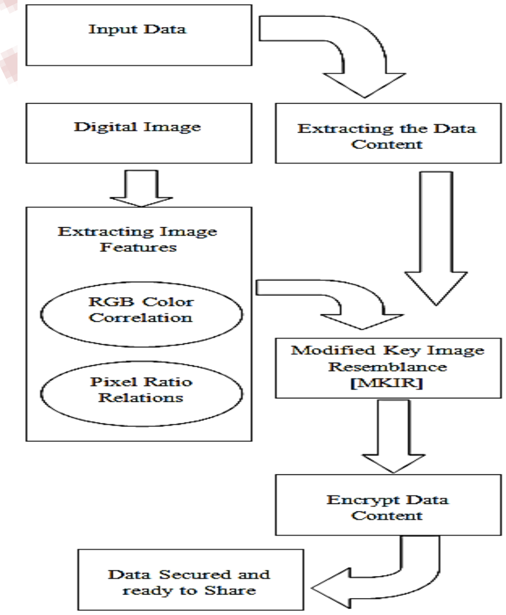

Input Data
Digital Image
Extracting the Data Content
Extracting Image Features
RGB Color Correlation
Pixel Ratio Relations
Modified Key Image Resemblance [MKIR]
Encrypt Data Content
Data Secured and ready to Share

Fig.1 Proposed System Architecture

The core of this approach is to generate the encryption methodologies by considering the image as the input key and the core features are extracted from the the image to encrypt the data, which is to be transmitted over the network. So this kind of logic processing is not easily guessable and processing complexity is high in precedence. This system of data processing and crypto feature assures the data to be more secure and safe in nature.

```
Algorithm: Modified Key Image Resemblance

Step-1: Input the Data with alpha-numeric features.
Step-2: Select the digital image to process.
Step-3: Extract the image features such as RGB color variance, pixel ratios, size of the image and so on.
Step-4: Manage the color variance of the digital images into matrix formatted indexing.
Step-5: Process Data and Image Pixels.
Step-6: Check for Pixel Ratio and Data length.
Step-7: Start iteration from oth position of the inputting text and up to the nth position of the text.
Step-8: Merge the data crypto keys with the actual keys and form a new key resemblance.
Step-9: Encrypt the data with the generated image key.
Step-10: Data Secured successfully with the new M-KIR key.
```

IV. EXPERIMENTAL RESULTS

The proposed algorithm has been implemented in MATLAB and experiments were carried out on wide number of inputs. The experimental results are very encouraging in terms of data security and integrity. To demonstrate the efficacy of the proposed algorithm, some sample results are presented here with few snapshots from the implemented matlab window. The following figure illustrates the input image.

Fig.2 Input Image

The following figure illustrates the selected resized portions of the input image.

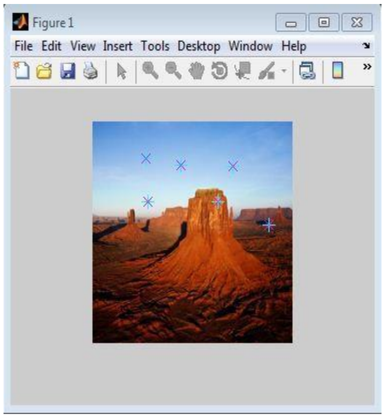
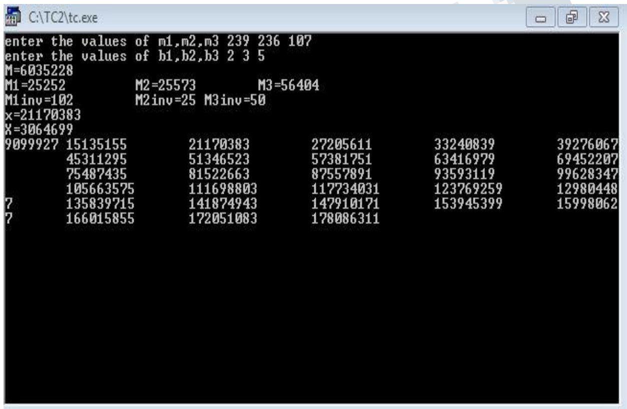


Fig.3 Resized Portion Selection of an Input Image

The following figure illustrates the generated key resemblance from the input image.



```
enter the values of m1,m2,m3 239 236 107
enter the values of b1,b2,b3 2 3 5
M=6035228
M1=25252        M2=25573        M3=56404
M1inv=102       M2inv=25 M3inv=50
x=21170383
X=3064699
9099927 15135155        21170383        27205611        33240839        39276067
        45311295        51346523        57381751        63416979        69452207
        75487435        81522663        87557891        93593119        99628347
        105663575       111698803       117734031       123769259       12980448
7       135839715       141874943       147910171       153945399       15998062
7       166015855       172051083       178086311
```

Fig.4 Generated Key Resemblance of an Input Image

In the proposed system of data encryption standard with image key crypto principles guarantees that the data is more safe and secured with this processing and the experimental results demonstrates that logic. The proposed algorithm of Modified Key Image Resemblance [MKIR] generates a 256-bit crypto key from the user's input image and process the data based on the input key and further generated the proper and secured encrypted text for transmission with recipient end. In case of security concern the nature of precedence is more strong and robust. As future norms, the data encryption principle is further improved by means of key simplified crypto principle logic.

V. CONCLUSION AND FUTURE SCOPE

The proposed system guarantees towards the data security and achieves the logic up to the end criteria, however, the data processing with 256-bit key logic is quite complex and time consumption is more. So, the further work might introduce some new logic to reduce the iterations and complexities in the proposed work.

REFERENCES

[1] Tetsuji TAKADA1 and Hideki KOIKE2, Awase-E: Image-based Authentication for Mobile Phones using User's Favorite Images

[2] Patra, Jagdish Chandra; Karthik, A, Bornand, Cedric, "A novel CRT-based watermarking technique for authentication of multimedia contents", Digital Signal Processing, Elsevier. DOI:http://dx.doi.org/10.1016/j.dsp.2009.07.004

[3] Ashraf Odeh, Aymen Abu-Errub, Mohammed Awad, "Symmetric Key Generation Method using Digital Image", International Journal of Computer Science Issues, Volume 12, Issue 2, March 2015, www.IJCSI.org

[4] Abdulrahman Dira Khalaf, "Fast Image Encryption based on Random Image Key", International Journal of Computer Applications (0975 – 8887), Volume 134 – No.3, January 2016

[5] QuisAphetsi Kester, " Image Encryption based on the RGB PIXEL Transposition and Shuffling", International Journal of Computer Network and Information Security, 2013, 7, 43-50, DOI: 10.5815/ijcnis.2013.07.05

[6] Chin Chen,Min-Shian, Tung -Shou "A new encryption algorithm for image cryptosystems", Elsevier's The Journal of Systems and Software 58(2001) 83-91,www.elsevier.co/locate/jss

[7] Seyed Mohammad Seyedzade, Reza Ebrahimi Atani, Rasht, "A novel image encryption algorithm based on hash function", Conference Paper • November 2010, DOI: 10.1109/IranianMVIP.2010.5941167 .Source: IEEE Xplore

[8] Ibrahim S I Abuhaiba1 and Maaly A S Hassan2, " Image Encryption Using Differential Evolution Approach in Frequency Domain" , An International Journal Signal

& Image Processing (SIPIJ) Vol.2, No.1, March 2011, DOI : 10.5121/sipij.2011.2105 51

[9] Qais H. Alsafasfeh, Aouda A. Arfoa, "Image Encryption Based on the General Approach for Multiple Chaotic Systems", Journal of Signal and Information Processing, 2011, 2, 238-244, Published Online August 2011,(http://www.SciRP.org/journal/jsip),doi:10.4236/jsip.2011.23033

[10] Lin Zhang , Lei Zhang ,David Zhang ,Hailong Zhu, "Online finger-knuckle-print verification for personal authentication" ,Journal of Pattern Recognition 43 (2010) 2560–2571,www.elsevier.com/locate/pr, doi: 10. 1016 /j. patco g .2010.01.020

[11] Ren Fujii, Yasunari Yoshitomi, Taro Asada, Masayoshi Tabuse, "Authentication Method Using a Discrete Wavelet Transform for a Digital moving Image", Journal of Information Security, 2016, 7, 1-13 Published Online January 2016 in SciRes, http:// www. scirp. org/ journal /jis.

[12] Stéphane Gael R. Ekodeck a,b,c , René Ndoundam, "PDF steganography based on Chinese Remainder Theorem" , journal of information security and applications (Elsevier) 29 (2016) 1–15