Abstract: - Crypto-Image systems are recently emerging in information security environment to address key management process. The conventional cryptographic key a random secret quantity used in crypto algorithms generated by the use of pseudo random process can result in security. This paper presents generation of cryptographic key using selected part of the image and with the mathematical concept of Chinese Remainder Theorem (CRT). The proposed method not only result to strong and secure cryptographic keys for symmetric encryption algorithms but also states that it is impossible for an attacker to guess or track the keys. Experimental results reports that variable length keys can be obtained based on the symmetric encryption algorithm employed during encryption and decryption of information.

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 approach 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 Integrity. Authentic is the term reveals the fact that the data is properly opened or accessed by the respective person and the term internetical 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/unscrembled. 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/secure. 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.

The below figure 1 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 unscrembled 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 bit-by-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 esteem. 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.

- Let $a_1$, $a_2$, ..., $a_n$ be pair wise relatively prime positive integers and let $b_1$, $b_2$, ..., $b_n$ be any integers. Then the system of linear congruence’s in one variable given by
  \[
  X \equiv b_1 \mod a_1 \\
  X \equiv b_2 \mod a_2 \\
  \vdots \\
  X \equiv b_n \mod a_n
  \]
  has a unique solution modulo $a_1 a_2 \ldots a_n$

Applications of Chinese Remainder Theorem
- Construction of Sequence numbering of Godel numbering uses the Chinese remainder theorem in the proof of Gödel's incompleteness theorems.
- Chinese Remainder theorem used in reduction in the computation of a Fast Fourier transform of size n1n2 to the computation of fast Fourier transforms of smaller sizes n1 and n2 by Good Thomas algorithm.
- Chinese Remainder Theorem used in most of the implementations of RSA during signing of HTTPS certificates and also used in secret sharing.
- One of the special applications includes techniques of Range ambiguity resolutions used with radar of medium pulse repetition frequency.
- The Method of Lagrange Interpolation, Fast Polynomial Multiplication etc… are some of the other applications.
VI. EXPERIMENTAL RESULTS

6.1 Key Generation Technique:
Cryptographic key has greater importance for any encryption algorithm. The success of any encryption algorithm depends on the key that is generated and used. Here we present the generation of cryptographic key from the selected portion of the image with the application of mathematical concept i.e Chinese Remainder Theorem. Initially, from the given set of images an image is selected. This selected image is used for the selection of portion on it with mouse. From the selected portion a number of pixel values are obtained that are represented in the form of matrix FV. Randomly certain predefined number of pixel values is picked from the matrix. Then relative prime condition is applied on the randomly picked values. CRT is assigned with these relative prime numbers as inputs and the output of CRT is the source for selection of key for any encryption algorithm.

6.2 Methodology of applying CRT onto the selected portion on RGB image to get variable length Key for Encryption Algorithm:

• **Step 1:** During encryption process, a set of RGB images are displayed, of which an image is selected.
• **Step 2:** On the RGB image, a portion is selected using mouse from which pixel values are obtained. These pixel values of selected portion of image is represented in the form of matrix Fv

  Matrix Fv, which represents the Red, Green, Blue pixel values as columns

• **Step 3:** From matrix Fv, randomly a set of number of non-zero pixel values are selected.

  \( M = \text{random}(F_v, x) \) where \( x \) is the number of values to be selected from matrix Fv.

• **Step 4:** Select N numbers from Fv of which say M1, M2, M3 from M are verified for relative prime condition.

• **Step 5:** For the CRT algorithm the above selected relative prime numbers are used as inputs. The result of CRT is \( P \) number of values which forms a source for random selection of variable length key. This variable length key which is randomly selected from P is used in information encryption and decryption process.

  \( P = \text{CRT}(M1, M2, M3) \) where M1, M2, M3 are inputs to CRT

  \( P \) means \( \{P1, P2, P3, P4 \ldots P_r\} \) where P is the result of CRT which forms a source for variable length keys P1, P2, P3...,Pr.

• **Step 6:** From the above steps, from a single selected image \( P_r \) number of values generated which are forming source for keys used in encryption algorithms. The total number of P values increases as the M values increases which are used as keys in symmetric encryption algorithms.

6.3 Experimental Results

• **Input:** An image selected from given set of RGB images

**Results:**

**Step 1:** Select a part of RGB Image using Mouse

![Original Image](image1.png)

Figure 1:- Original Image used to select a part on the image with mouse
**Step 2: Matrix from Selected part on RGB Image**

Final Matrix $F_v$

Cropped Image $(::,1) =$ 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|
|255|254|255|255|255|255|233|246|255|255|254|240|232|246|243|245|
|252|255|255|252|255|252|231|252|254|255|241|235|242|245|250|
|255|254|254|255|253|244|233|255|254|255|238|235|246|247|255|
|254|255|255|253|255|238|246|255|255|254|248|238|244|252|253|255|
|255|255|255|255|254|240|254|255|255|254|244|242|249|252|255|253|
|252|254|254|255|243|241|254|254|255|253|242|246|250|253|255|
|255|253|255|254|255|240|247|255|255|255|245|245|247|252|255|255|
|255|253|255|253|253|253|254|255|255|253|245|252|251|251|255|255|
|254|255|255|254|249|245|255|253|253|254|245|244|252|255|255|253|
|255|253|255|242|250|253|255|255|254|249|241|242|242|251|254|255|248|
|255|254|255|237|254|255|253|243|240|245|245|249|255|254|249|
|253|255|248|247|255|255|255|240|239|245|252|251|252|255|251|
|255|254|250|250|254|255|254|252|239|245|245|245|254|255|255|244|
|254|255|239|252|255|255|243|241|245|246|251|255|253|253|244|
|253|252|242|255|254|252|237|241|246|251|251|255|254|250|246|
|255|248|249|253|255|255|246|239|240|244|251|251|254|255|247|244|
|255|246|255|255|253|255|245|241|244|246|250|255|253|254|245|243|
|251|243|255|255|255|252|241|246|248|247|255|254|255|249|239|248|
|249|244|255|255|255|248|238|246|253|252|255|253|256|246|240|254|
|247|251|254|255|255|242|239|249|254|251|255|254|243|245|252|
|243|255|254|255|253|240|245|250|255|255|253|251|241|248|246|
|243|255|255|255|248|245|247|252|254|253|255|244|239|249|240|
132 136 142 141 140 139 105 61 54 68 82 78 19 8 4 3
133 142 145 136 137 137 101 67 64 75 89 71 14 8 4 3
180 207 197 179 176 181 110 72 75 84 92 56 12 6 6 4
226 251 228 221 233 218 113 72 79 89 91 43 11 4 6 6
238 248 227 225 244 198 97 74 81 93 85 32 11 8 7 12
245 240 222 236 247 164 89 78 81 94 71 23 11 16 14 17
250 233 221 243 234 130 79 83 85 94 55 17 10 12 17 26
248 229 226 250 211 104 79 84 92 88 34 14 13 14 21 26
245 226 233 249 170 87 84 89 96 71 22 16 15 17 23 25
238 226 239 230 139 82 86 87 91 54 18 12 14 17 25 22
225 225 245 208 112 84 84 91 83 36 16 13 13 21 24 25
222 229 246 180 97 86 81 93 75 27 11 10 17 23 25 23
225 237 236 146 86 84 87 93 54 19 14 11 18 22 24 17
229 244 217 116 85 83 88 85 35 13 13 13 19 22 18 14
232 241 180 97 84 86 90 71 19 13 13 15 18 21 17 13
235 233 156 92 86 88 93 51 18 13 14 17 17 18 16 17
241 219 124 91 87 87 82 35 15 11 15 18 22 20 15 12
246 194 103 90 85 88 67 23 13 12 15 18 20 21 14 7
241 160 95 88 88 88 45 20 12 12 15 15 17 20 15 10
223 128 92 92 81 32 15 14 14 14 20 18 16 13 16
197 108 89 90 92 69 22 16 12 14 19 19 20 20 13 24
163 96 87 89 87 52 19 12 13 17 18 16 17 14 14 31
130 90 89 95 79 32 13 10 14 18 19 18 16 11 15 40
111 90 89 91 63 20 14 14 13 14 17 15 15 8 22 55
100 89 88 86 46 18 14 16 14 19 16 18 10 11 30 85
96 89 90 79 31 15 12 14 16 20 19 20 12 18 35 136
92 87 89 63 19 15 13 14 15 16 19 18 11 24 53 189

Columns 17 through 31
2 0 0 2 1 23 154 216 212 208 197 198 205 198 200
0 1 2 3 4 16 132 218 212 209 207 205 209 208 201
0 3 3 1 8 14 116 216 211 211 209 207 209 212 210
1 2 1 1 6 15 110 220 215 215 210 211 212 214 214
2 4 4 4 8 15 107 226 220 215 210 212 215 218 213
2 1 2 6 7 14 106 232 224 218 211 209 215 221 220
2 1 0 1 3 13 110 235 227 223 213 208 214 227 224
4 4 4 4 7 10 112 238 229 221 213 204 221 228 228
6 4 8 5 5 13 110 237 230 225 214 213 225 227 229
5 4 8 9 8 17 122 236 232 229 216 222 232 231 231
7 7 9 8 11 22 145 245 237 225 215 225 233 238 232
10 9 8 9 11 27 170 252 235 221 217 227 240 243 233
14 16 11 11 11 37 193 248 235 217 223 231 243 247 233
19 16 13 11 15 58 219 244 232 219 228 235 247 247 238
25 19 10 11 21 96 239 244 230 220 228 238 250 245 241
23 16 10 13 32 141 250 241 231 223 231 244 251 247 247
23 15 9 18 37 177 252 242 228 230 239 246 248 246 247
18 14 12 19 64 221 254 247 228 233 243 248 247 246 239
17 17 13 19 116 245 249 247 231 235 240 247 246 235
18 16 12 33 169 254 249 238 226 236 247 250 245 245 234

DOI: 10.21817/ijet/2017/v9i4/170904051
Vol 9 No 4 Aug-Sep 2017
2936
croppedImage(:,:,3) =
Columns 1 through 16
15 34 0 2 1 0 0 0 0 1 1 0 0 1 0 0
0 0 4 0 0 2 1 0 0 1 3 0 0 0 0
0 2 2 0 3 2 0 1 2 0 0 0 0 0 3 4
0 0 1 0 1 2 0 2 0 0 2 4 0 2 4
0 3 2 0 2 0 0 0 0 0 2 4 0 2 0
0 0 0 0 0 2 2 0 1 1 0 0 2 0 2
0 2 0 0 3 0 1 0 0 1 1 8 0 0 2 0
0 0 1 2 0 1 0 1 0 3 0 17 3 0 0 3
0 0 0 1 0 0 1 0 1 0 6 10 0 0 1 0
0 0 1 0 4 2 2 2 0 8 8 0 0 0 0
25 60 41 14 14 35 4 1 0 2 13 7 1 1 1 1
72 112 79 61 78 79 3 1 4 10 12 0 2 2 0 1
77 95 58 48 82 50 0 0 2 2 8 2 0 0 0 2
85 79 43 59 87 23 3 0 2 3 3 2 0 1 0 5
91 65 38 68 70 6 0 0 3 6 0 0 3 0 3 11
82 54 41 84 57 2 0 4 7 10 1 1 0 2 2 7
79 41 54 92 29 1 0 0 5 5 0 3 0 2 7 7
62 35 57 62 9 2 1 0 4 1 0 0 0 0 10 5
46 37 67 44 2 1 0 6 6 0 2 1 1 4 10 9
43 44 73 25 0 1 0 5 8 0 0 1 0 3 10 7
39 53 72 8 0 0 2 8 0 0 1 1 1 2 8 0
44 59 54 1 0 0 2 10 0 0 0 0 4 5 4 0
45 62 19 2 0 0 4 7 0 1 0 0 3 5 4 1
54 56 8 1 0 0 5 5 0 1 0 0 5 2 3 1
66 50 0 1 0 2 5 0 0 0 0 1 8 13 5 0
70 32 0 1 0 4 3 0 0 3 1 3 6 6 3 0
64 11 0 0 0 5 0 1 0 0 1 1 1 3 1 0
48 2 1 1 1 2 2 0 1 0 0 3 1 3 1 0
29 0 0 2 1 3 2 0 0 0 5 2 3 1 1 0
14 0 0 0 7 4 0 1 0 0 5 0 4 4 0 0
1 2 0 1 4 0 0 5 1 1 6 5 3 1 0 0

ISSN (Print) : 2319-8613
ISSN (Online) : 0975-4024
Kalyanapu Srinivas et al. / International Journal of Engineering and Technology (IJET)

DOI: 10.21817/ijet/2017/v9i4/170904051
Vol 9 No 4 Aug-Sep 2017
2937
Step 3: The above numbers are checked for relative prime condition

OUTPUT:-

M1 = 237, M2 = 208, M3 = 253 are RELATIVE PRIME NUMBERS

OTHER POSSIBILITIES:-

M1 = 87, M2 = 208, M3 = 253 are RELATIVE PRIME NUMBERS

M1 = 57, M2 = 208, M3 = 253 are RELATIVE PRIME NUMBERS
M1 = 57, M2 = 13, M3 = 22 are RELATIVE PRIME NUMBERS

**Step 4:** Above relative prime numbers are taken as inputs to CRT and the output of CRT is P number of values which forms a source for random selection of variable length key are as shown.

**OUTPUT:**

![CRT Output](image)

Figure 3.: CRT Output for the given inputs

As an example one of the randomly selected numbers from Step V is the key used in Encryption algorithms say DES algorithm

![DES Algorithm](image)

Figure 4.: Implementation in DES Algorithm

**VII. CONCLUSION AND FUTURE SCOPE**

The prior research perceived the shortcomings of essential authentication plans. A Survey led from customary secret word and PIN validation to image validation framework delineates that confirmation frameworks have potential applications and these frameworks are well reasonable to some degree however with a few disadvantages. In this approach different image confirmation plans were broke down by which obviously application arranged validation techniques are proposed. Generally applications need to endure some image controls ascending to new challenges sitting tight for validation group. Truth be told, a few calculations offer high resilience exhibitions against controls that are particular to applications which incorporate pressure, geometrical changes sifting and so forth. Be that as it may, even to be strong against a predefined set of controls an enhanced hash work strategies with a blend of qualities of change are to be proposed. The best eminent and identifiable elements removed from each approach are appeared earlier. Every procedure is one of a kind in its own particular manner, which is appropriate for various applications.

This contextual investigation gives data of points of interest what's more, hindrances of various security strategies to the future designers to propose a more clever strategy utilizing images. In future upgrades this approach helps in separating abnormal state qualities to be utilized as a part of validation strategies that would be powerful against the image controls. Ordinary new encryption systems are advancing thus quick and secure regular encryption strategies will dependably work out with high rate of security.
REFERENCES

Books:-
[1] Cryptography and Network Security by William Stallings.
[2] Network Security Essential by William Stallings

Papers:-
[1] Jiri Fridrich, “Image Encryption Based on Chaotic Maps”, Proceeding of IEEE Conference On Systems, Man, and Cybernetics, pp. 1105-1110, 1997.
[2] Jui-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.
[3] Jui-Cheng Yen, and Juan-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.
[4] M.I.Sobhy, and A.R.Shehata, “Chaotic Algorithms for Data Encryption”, IEEE Proceeding of ICASSP 2001, Vol 2, pp.997-1000, May. 2001.
[5] 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.
[6] 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
[7] 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.
[8] Fethi Belkhouche and Uvais Qidwai, "Binary image encoding using 1D chaotic maps", IEEE Proceeding in the year 2003.
[9] 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
[10] 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
[11] 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.
[12] Huang-Pei Xiao Guo-Ji Zhang “An Image Encryption Scheme Based On Chaotic Systems”, IEEE Proceeding of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.
[13] Guosheng Gu Guoqiang Han “An Enhanced Chaos Based Image Encryption Algorithm”, IEEE Proceeding of the First International Conference on Innovative Computing, Information and Control (ICICIC’06) in 2006.
[14] H. Cheng and X. Li, “Partial Encryption of Compressed Images and Video," IEEE Transactions on Signal Processing, 48(8), 2000, pp. 2439-2451.
[15] 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.
[16] 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.
[17] IEEE Transactions on Circuits and Systems for Video Technology: Special Issue on Authentication, Copyright Protection, and Information Hiding, Vol. 13, No. 8, August 2003.
[18] 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.

AUTHOR’S BIOGRAPHY

Kalyanapu Srinivas, Ph.D. Scholar at the Department of Computer Science and Engineering of the JNTU University. He is now working as Assistant Professor in CSE Department, SR Engineering College, Warangal and a member of the Computer Society of India and ISTE Society. His research interests include Network security and cryptogrophy, Image processing’s, Biometrics, Pattern Recognition, Computer Vision, etc.

Dr. V. Janaki Professor, and HOD of CSE Department, Vaagdevi Engineering College, Warangal. She received her PhD in Computer Science and Engineering from JNT University, Hyderabad, Telangana, India. Her research interests are related to information security, and in computer networks. She had published 30 above technical research papers in various National/International Journals and Conferences.