ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

A Novel Encryption and Compression Technique for Efficient Data

Daundkar Anita Mohan, Pratima Bhati

Master of Engineering, Dept. of Computer Engineering, Dhole Patil College of Engineering, Wagholi, Pune, India

Professor, Dept. of Computer Engineering, Dhole Patil College of Engineering, Wagholi, Pune, India

ABSTRACT: The practical scheme describe that, encryption of image has to be attend before the compression of image. But for such scheme there establish a problem that how to design an image encryption and after that compression algorithms so that there are efficiently compress the encrypted image. For that, this project develop an image encryption-then-compression (ETC) system which is highly efficient, in that there consider both lossless and lossy compression. In proposed system, for image encryption and decryption scheme use of the color and whole number which is to be capable to provide security with very high level. And there is better compression of encrypted images and also perform efficient decompression with the algorithms like Huffman algorithm, The Shannon Fano Compression Algorithm.

KEYWORDS:Encryption of image by color and whole no, Compression, Decryption, De compression.

I. INTRODUCTION

Suppose there is a scenario in that, Charlie is untrusted channel provider and through a Charlie, the owner of information Alice need to transmit securely and efficiently to a recipient Bob. This above process will arrive as follows. Alice first compress I to B, after that he encrypt B into I_e with the help of Encryption FunctionE_K (.), where K is the secrete key, which is shown in Fig. 1. After performing encryption, the encrypted data is given to Charlie. After that Charlie simply forward this information to Bob. Then first Bob decrypt information with the help of decryption and then decompress the decrypted information using decompression which get original image Iˆ.

Despite if the above Compression-then-Encryption (CTE) example satisfy the requirements in many secure transmission situation, the sequence of applying the compression and encryption required to be opposite in some different conditions. Even if through encryption method the data owner Alice is every time interested in protecting the secrecy of the image information. Then, Alice has no need to compress her data, and hence, to run a compression algorithm before encrypting the data, will not use her limited computational resources. This will be true for the use of resource-deprived mobile device. The channel provider Charlie compress the data if load on the channel increases to increase the network utilization. So that data which is already compressed which again compress by channel provider. So that it will be better if the operation of compression performed by the channel provider who has copious computational resources. The big challenge with the Encryption-then-Compression (ETC) framework is that the compression has to be performed on the encrypted data, so that network provider Charlie does not provide cannot access the secrete key K. The ETC system is express in Fig.2 [1]

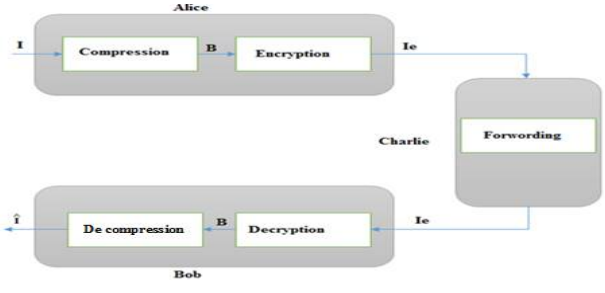

Fig. 1. Traditional Compression-then-Encryption (CTE) system [1]

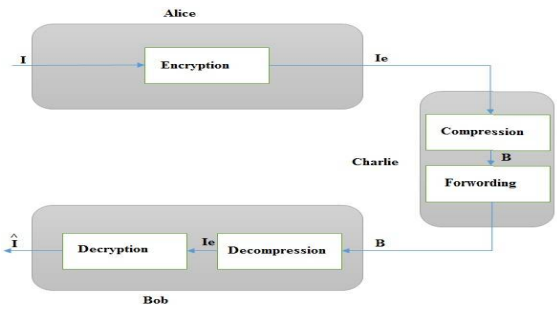

Fig. 2. Encryption-then-Compression (ETC) system [1].

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Today, different methods are used to make secure data transmission. One of the techniques is Cryptography. In Cryptography, the simple data is converted into indecipherableform and again get back it in original form using the encryption and decryption process. In proposed system is the Security Using Whole Numbers with Color. In that the first step is to authorize a different color for each recipient. Set of three values represented with each color. For example In RGB format (238, 58,140) is represented by violet red color. In the next step a set of three key values are assign to each receiver. At Sender and Receiver ends the data is present. The sender know about the required receiver to which the data will have to send. So as the password, the receiver's unique color is used.

In the color value the set which has three key values are added and encrypted at the sender's side. As a password use this encrypted color. Using Whole numbers the actual data is encrypted. The receiver known his own color and key value. At the receiver's side, the key values are subtracted from actual color value and decrypt the encrypted color. Then receiver send that decrypted color send to the sender for matching. If that color match with senders color then using Whole number the actual data decrypted.

II. RELATED WORK

Encrypted Domain DCT based on homomorphic Cryptosystem by Tiziano Bianchi [2] describes Signal processing in the encrypted image Discrete cosine Transform (DCT) tool is used to process encrypted data. Homomorphic encryption is a form of encryption which allows specific types of computations to be carried out on cipher text and generate an encrypted result which, when decrypted, matches the result of operations performed on the plaintext. This is a desirable feature in modern communication system architectures. Homomorphic encryption would allow the chaining together of different services without exposing the data to each of those services, for example a chain of different services from different companies could 1)calculate the tax 2) the currency exchange rate 3) shipping, on a transaction without exposing the unencrypted data to each of those services. DCT allows a large no of processing tasks to be carried out on encrypted images like extraction of encrypted data from encrypted image, embedding watermarking in encrypted image etc. Different types of DCT method: 1D DCT, 2D DCT, CD BDCT(block based DCT). DCT performs the operation on image like The disadvantage of this method is Most of the computation time required to transform, quantize, dequantize, and reconstruct an image is spent on forward and inverse DCT calculations. Because these transforms are applied to blocks, the time required is proportional to the size of the image These times are much longer than for comparable functions written in a low-level language such as C. Size of the image get increases after decryption.

Privacy Preserving ECG Classification with Branching Programs and Neural Networks by Mauro Barni [5] describes Privacy protection is a crucial problem in many biomedical signal processing applications. For this reason, particular attention has been given to the use of secure multi- party computation techniques for processing biomedical signals, whereby nontrusted parties are able to manipulate the signals although they are encrypted. This paper focuses on the development of a privacy preserving automatic diagnosis system whereby a remote server classiest a biomedical signal provided by the client without getting any information about the signal itself and the nil result of the classification. Systems prove that carrying out complex tasks like ECG classification in the encrypted domain efficiently is indeed possible in the semi honest model, paving the way to interesting future applications wherein privacy of signal owners is protected by applying high security standards. Disadvantages of this paper is complexity is very high.

On Compression of Data Encrypted With Block Ciphers by DemijanKlinc, based on Slepian-Wolf coding and hinges on the fact that chaining modes, which are widely used in conjunction with block ciphers, introduce a simple symbol- wise correlation between successive blocks of data.in communication systems, data from a source is first compressed and then encrypted before it is transmitted over a channel to the receiver. While in many cases this approach is befitting, there exist scenarios where there is a need to reverse the order in which data encryption and compression are performed. Consider for instance a network of low-cost sensor nodes that transmit sensitive information over the internet to a recipient. The sensor nodes need to encrypt data to hide it from potential eavesdroppers, but they may not be able to perform compression as that would require additional hardware and thus higher implementation cost. The compression was shown to preserve the security of the encryption scheme. the existence of a fundamental limitation to compressibility of data encrypted with block ciphers when no chaining mode is employed. But this method is theoretically well suited but practically implementation not works properly.

Security Using Colours and Armstrong Numbers by S. Pavithra uses the Armstrong no and colour as encrypted key for data protection.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

III. PROPOSED SYSTEM

Proposed System uses color and whole number to encrypt the data and then this data is compressed. Primary focus is on practical design of a pair to process the encryption and compression methods in such a way that there are efficiently done the encrypted image compression and compressing the unencrypted original image is equally efficient. Due to high sensitivity encryption and compression there obtain high level of security could be reasonably.

Proposed Approach:

System assign the ASCII equivalent to the characters, this is the substitution process. Using matrices and Whole number the process is complete. The first step of this technique is to appoint a different color for each and every receiver. Set of three values are represented with each color. For example in RGB format as (238, 58,140) is represented by violet red color. In the next step a set of three key values assign to each receiver.

Common database of the sender date stored at each receiving end the sender is known about the required receiver. So that as a password use the receiver's unique color. The original color values are added with the set of three key values and then encrypted at the sender's side. Then as a password use this encrypted color. Then using Whole numbers actual data is encrypted.

The receiver is known his own color and also other key values at the receiver's side. At receiver side the receiver decrypt the color which is encrypted by the sender by subtracting the key values from the color value. Then it is matched with the color which is stored at the sender's database. The certain information decrypted with the help of Whole numbers only when the colors are matched. For surety of maximum security to the information providing, for authentication usage of colors as a password. This is because the actual data could be accessed after matching the colors at sender and receiver's side with each other

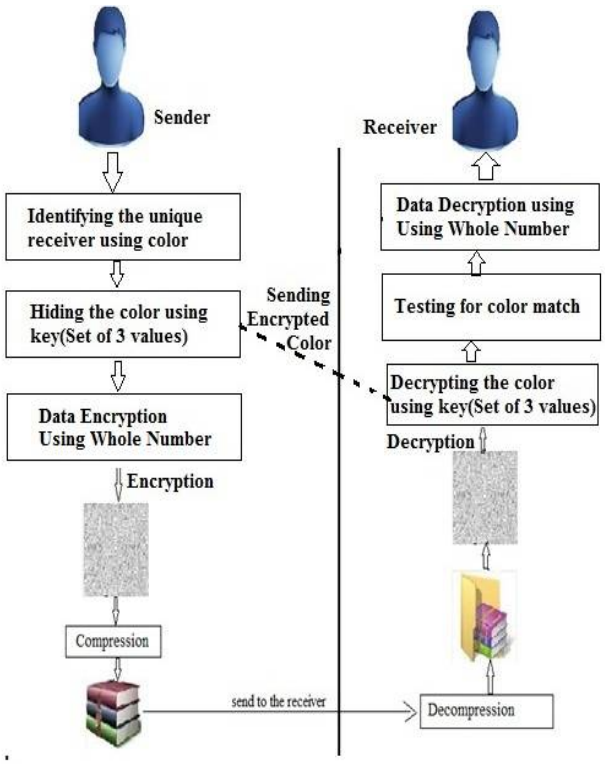

Fig 3 .Layout of the proposed technique

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

IV. PROPOSED ALGORITHM

1) Encryption:
Assume that the information which has to be send to the receiver (say A) which the color (120, 35, 20) is assigned. Let with this color value the key value (10,3,4) to be added. And let the Whole number 153 be used for data encryption.

Step 1: (Password creation)
Initially the sender knows about the required receiver which is to be A. So that the some color values are appoint for receiver A, and the key values are added.

120 35 20
+10 3 4
---
130 38 24

Now for security check, a newly encrypted color is designed.

Step 2: (Actual data Encryption)
Let the transmitted message be "SECURITYTECH". Then find ASCII equivalent values of the above all characters.

S E C U R I T Y T E C H
83 69 67 85 82 73 84 89 84 69 67 72

Step 3: Now perform addition of the digits of the Whole number with these numbers as follows

83 69 67 85 82 73 84 89 84 69 67 72
(+) 3 7 1 9 49 1 27 343 1 3 7 1
---
86 76 68 94 131 74 111 432 85 72 74 73

Step 4: Then, convert the above data into a matrix form as follows

$$A=\begin{bmatrix} 86 & 94 & 111 & 72 \\ 76 & 131 & 492 & 74 \\ 68 & 74 & 85 & 73 \end{bmatrix}$$

Step 5: Now, consider an encoding matrix...

$$B=\begin{bmatrix} 3 & 7 & 1 \\ 9 & 49 & 1 \\ 27 & 343 & 1 \end{bmatrix}$$

Step 6: Then, perform multiplication of two matrices (B X A) we get

$$C=\begin{bmatrix} 858 & 1273 & 3442 & 807 \\ 4566 & 7339 & 22252 & 4347 \\ 28458 & 47545 & 151258 & 27399 \end{bmatrix}$$

After multiplication, encrypted data is generated which is,
858,4566,28458,1273,7339,47545,3442,22252,151258,807,4347,27399
The above values are the encrypted mode of original information. Step [2-6]

2) Compression:
After encryption sender send the encrypted data to the service provider. If there is more traffic on the server, then service provider compress this encrypted data to minimize the traffic on the server. After that, he send this compressed data to the receiver.But, if there is less traffic on the server then there is no need to compress the data. So that service provider directly send the encrypted data to the receiver without compressing it.There are different algorithms for compression are provided to network service provider for effective utilization of bandwidth. Algorithms like Huffman, The Shannon FanoCompression Algorithm, Run-length encoding (RLE) etc. can be used

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

3) Decompression:
In this process, there is must to decompress the data which is compressed by the service provider. But, if data was not compressed by the service provider, then there is no need to decompress it.

4) Decryption:
After decompression, the receiver decrypt this data. The process retake original information back using decryption key. Then sender's end data is matched with the data which is given by the receiver (the color). The receiver must be aware of the key values and his own color being assigned for this process.

Step 1: (The receiver Authentication)
The actual color being assigned is (120, 35, 20) for the receiver A (as assumed), the original color can get back by subtracting the key values from the color value.
The decryption process is as follow:

```
 130   38   24      Accepted data
-10    3    4       values of key
-----------------------------------
120   35   20
```

The data stored at the sender's side, the above set of values (135, 38, 87) is compared. The original data can get back by performing following steps, only when they both match.

Step 2:(Original data Decryption)
Take the inverse of the encoding matrix
D=B^{-1}

$$D = \begin{bmatrix} -7/24 & 1/3 & -1/24 \\ \frac{1}{56} & -1/42 & 1/168 \\ 7/4 & -5/6 & 1/12 \end{bmatrix}$$

Step 3: Now perform multiplication of decoding matrix and the encrypted data matrix i. e. (D X C), we get

$$D \times C = \begin{bmatrix} 86 & 94 & 111 & 72 \\ 76 & 131 & 492 & 74 \\ 68 & 74 & 85 & 73 \end{bmatrix}$$

Step 4: Then the above result transform as given below
86 76 68 94 131 74 111 432 85 72 74 73

Step 5: Now, Subtract Whole numbers from the digits as follows

```
  86 76 68 94 131 74 111 432 85 72 74 73
(-) 3 7  1  9  49  1   27  343 1  3  7  1
-----------------------------------------------------------------
83 69 67 85 82 73 84 89 84 69 67 72
```

Step 6: From the above ASCII equivalent obtain the characters from step[2-5]
83 69 67 85 82 73 84 89 84 69 67 72
S E C U R I T Y T E C H.

V. RESULTS

In this, there uses color and whole number for encrypt data at sender side. For that, first the image taken to generate the key. After the key generation the RGB values taken from selected color. Then that RGB values and key values are added to generate the secrete key. Then this secrete key send to the receiver. After that take the data which will have to send to the receiver. By using whole number that data will be encrypted. And generate the output as follows.

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Fig.4 Original Image

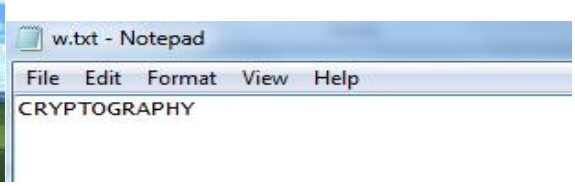

Fig.5. Original data

Generated key is shown in fig 6 as below.

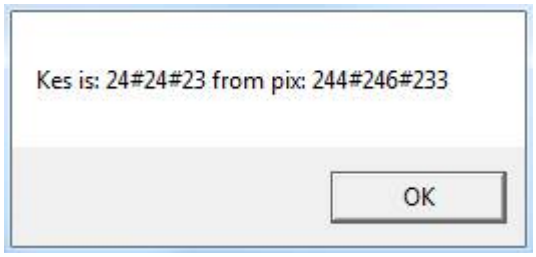

Fig 6 Generation of key from color pixel

Images after encryption shown in fig7 and fig 8.

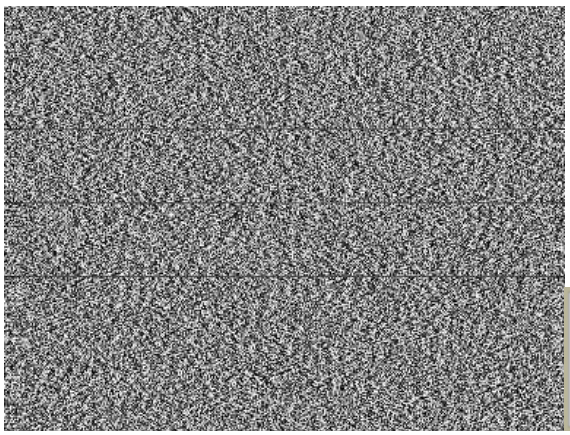

Fig7. Encrypted Image

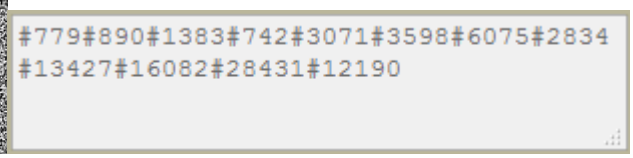

Fig8. Encrypted Data

Fig 4 and Fig 5 are the input data on which encryption operation is performed. Using whole number and color secrete key generated. The output data after encryption as fig7 and fig8 respectively. At NSP compression operation is takes place for effective bandwidth utilization.

VI. CONCLUSION AND FUTURE WORK

In proposed system, for image encryption and decryption scheme uses the color and whole number which is to be capable to provide security with very high level. And there is better compression of encrypted images and also perform efficient decompression. In military, the above combination of public key and secrete key cryptography can be applied

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

because, more importance is for security of data. When the length of the key of the whole numbers increase, then this technique provides more security. Thus by the use whole numbers, additional set of key values and colors in this technique there is surety that the data is deliver securely and that only authorized peoples can access it.

REFERENCES

1. J. Zhou, X. Liu, and O. C. Au, "On the design of an efficient encryption then-compression system," in Proc. ICASSP, 2013, pp. 2872–2876.
2. T. Bianchi, A. Piva, and M. Barni, "On the implementation of the discrete Fourier transform in the encrypted domain," IEEE Trans. Inf. Forensics Security, vol. 4, no. 1, pp. 86–97, Mar. 2009.
3. T. Bianchi, A. Piva, and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems," EURASIP J. Inf. Security, 2009, Article ID 716357
4. T. Bianchi, A. Piva, and M. Barni, "Encrypted domain DCT based on homomorphic cryptosystems," EURASIP J. Inf. Security, 2009, Article ID 716357
5. M. Barni, P. Failla, R. Lazzeretti, A.-R. Sadeghi, and T. Schneider, "Privacy-preserving ECG classification with branching programs and neural networks," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 452–468, Jun. 2011.
6. Z. Erkin, T. Veugen, T. Toft, and R. L. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," IEEE Trans. Inf. Forensics Security, vol. 7, no. 3, pp. 1053–1066, Jun. 2012.
7. M. Johnson, P. Ishwar, V. M. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol. 52, no. 10, pp. 2992–3006, Oct. 2004
8. D. Schonberg, S. C. Draper, and K. Ramchandran, "On blind compression of encrypted correlated data approaching the source entropy rate," in Proc. 43rd Annu. Allerton Conf., 2005, pp. 1–3.
9. S. Pavithra Deepa,S. Kannimuthu, V. Keerthika., "Security Using Colors and Armstrong Numbers", Proceedings of the National Conference on Innovations in Emerging Technology-2011. India.17 & 18 February, 2011.pp.157-160.
10. Chavan Satish, Lokhande Yogesh, Shinde Pravin, Yewale Sandeep, Sardeshpande S. A, "Secure Email using Colors and Armstrong Numbers over web services",International Journal Of Research In Computer Engineering And Information Technology VOLUME 1 No. 2