Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 6, June 2014, pg.432 – 437

RESEARCH ARTICLE

A Random Key Based Visual Cryptography Approach for Information Security

Aruna Tomar
Student, Electronic & Communication Engineering Department
DCR University of Science & Technology, Murthal (HR), India
aruna_tomar07@yahoo.com

Sunita Malik
Asstt. Prof., Electronic & Communication Engineering Department
DCR University of Science & Technology, Murthal (HR), India
sntmlk76@gmail.com

***Abstract*— The cryptographic mechanism basically secures the data while performing the information distribution in an open environment. According to type of data, application or the user, different kind of secure cryptographic approaches are available. In this paper, different types of cryptographic approaches are discussed. The efficiency of these approaches depends on the message size and the key size. In this paper, one of the most effective cryptography approach called Random Key cryptographic is discussed. The paper has defined the algorithmic approach adapted by the approach along with result analysis. The obtained results from the system shows the Random key Visual Cryptography is effectively efficient.**

***Keywords*—RSA, Random Key Visual Cryptography, Key-Size, Message-Size**

I. INTRODUCTION

To perform the secure and reliable communication over the network, there are number of available approaches such as Visual Cryptography, steganography, watermarking etc. One of such most reliable and data oriented scheme is Visual Cryptography. Visual Cryptography is about to encode different kind of data so that undesirable person will not recognize the information. The cryptographic approach is based on information type such as images, text, audio, video etc. Visual Cryptography basically saves the information from any kind of active attack that is performed by attacker to reveal the information. Cryptography prevents the unauthorized access on data. Cryptographic process is itself divided in two stages called encryption and decryption. Encryption is about to convert the information in encoded unreadable and unrecognizable form whereas the decryption process is reverse to that. It actually converts the encoded information to its actual form. To provide the authorization of communication evolving parties, some authentication key is incorporated the cryptographic information. Number of keys depends on the level of security involved. In case of simplest form of cryptographic structure, single symmetric key is used to encode and decode the data. Such cryptographic approach is called private key Visual Cryptography. To restrict the operation performed on sender and receiver side, some complex Visual Cryptography approach is required. One such approach is public key Visual Cryptography in which encoding

and decoding process is performed by separate keys. If more than one person is involved in cryptographic operation with equal data contribution, then to maintain the trust level, the concept of shared key is used. In case shared key, multiple key are accepted from different user and generate a single key to perform the cryptographic operation. The shared key can be public or private. Here in figure 1 some of the important cryptographic approaches are shown in figure 1.

The above define cryptographic approaches are the standard cryptographic forms that covers the maximum usage of information encoding. Other than these some more cryptographic approaches are used to cover the challenges associated with cryptographic approaches. Once such cryptographic approach is location based Visual Cryptography. This cryptographic approach is used to secure the data from social hacking. As the name suggest, this cryptographic approach uses the location key for sender and receiver identification. It means, to open the cryptographic location, the racier must be available at the particular location specified as the cryptographic key. The location information key is been used for cryptography [8] [9].

Another aspect of cryptographic approach is presented by geographical Visual Cryptography. In this approach, data is encoded to some geographical shape initially. Once the data is encoded to this form, the next work is to perform the geographical transformation on this shape data to perform the information encoding. Geographical cryptographic uses the graphical aspects for encoding and key specifications. Another complex form of Visual

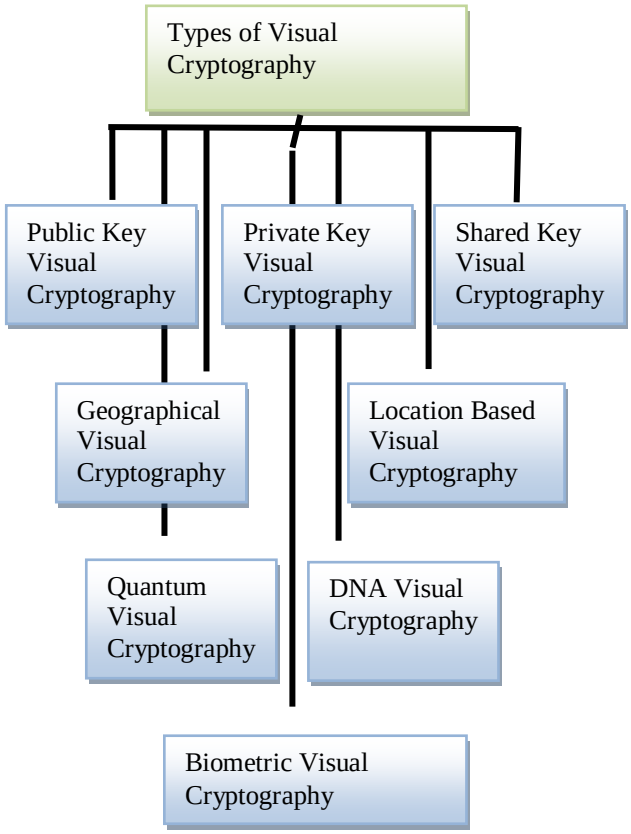

Figure 1 : Types of Visual Cryptography

Cryptography is the quantum key Visual Cryptography. Quantum is used to provide the high level security for high speed servers where layered Visual Cryptography is performed under the quantum law of encoding. This kind of encoding approach uses the mathematical integrated aspects to encode and decode the information. Another cryptographic approach used in last few years is to encode the data based on the biometric features of the sender or the receiver. It means the key is extracted from any of the human feature such as fingerprint, sign, face etc. Now while extracting the information back, same key is required. The personal authenticated keys are used to gain the person specific security. One more cryptographic approach adapted in many secure communication approaches is the DNA Visual Cryptography. DNA is the most advanced form of information representation. In this form, the DNA patterns or the sequence is considered as the generation of the key [11] [12] [13] [14].

In this paper, an effective random key cryptography approach is presented to enhance the visual cryptography. In section I, the introduction to the cryptographic concepts and the description of some of some of the available cryptographic approaches and their categorization is given. In section II, the work defined by the earlier authors is defined. In section III, the algorithmic approach adapted by random key cryptography is explained in section IV, the results obtained from the work are discussed. In section V, the conclusion obtained from the work is presented.

II. RELATED WORK

In this section, the work defined by the earlier authors is discussed. With the beginning of digital data communication, the side effects of this kind of communication are identified in terms of information leakage. To prevent this kind of information loss, there are number of cryptographic approaches suggested by different researchers. The main theory of Visual Cryptography represented as the security principle, was presented by Kerchhoff[5]. Author designed cryptosystem to secure the information. As the earlier approach, author observed the requirement of the Visual Cryptography and to involve the number of person in the cryptographic Approach. According to this approach, the receiver knows about the algorithmic approach used for the Visual Cryptography. But it gives the information leak and the information insecurity. Because of this, there was the requirement to secure the information without revealing the cryptographic algorithm. Because of this, the cipher text cannot get cracked in the absence of algorithmic approach [2].

Another main aspect of cryptographic process is the Visual Cryptography key. Key is the actual mutual information used by the sender and receiver to secure the information. There are number of adaptive approaches to reduce the key size and space. One of such approach was defined by [3]. Author concluded that the large key size increases the security level. The key generation is also based on the key space or the data range on the basis of unique keys can be generated. Author observed that as the key length increases, the information decoding becomes more complex. Author discussed different aspects of cryptographic key such as key length, key sharing, key generation etc.

Based on these parameters, there are number of cryptographic approaches defined by different researchers. Author [4] discussed the concept of symmetric and asymmetric key Visual Cryptography. Author discussed the key based algorithms so that the effective security and reliability to system will be achieved. One of such cryptographic approach was discussed by the author[5] called Triple DES approach. In this cryptographic form 168 bit key is used to encode the information. This cryptographic approach is based on the cryptographic algorithm and the comparative algorithm with some other cryptographic algorithms is also defined [5] [6]. Another important concept with cryptographic data communication is the cryptanalysis. It is basically used by the attackers or crackers to reveal the information from encoded data. As the data access is performed by unauthorized person, so that the data extraction is performed without the knowledge of cryptographic key. This information extraction is considered as the integrity attack over data [7] [8].

III. PROPOSED APPROACH

As discussed in earlier sections there are number of cryptographic approaches available to secure the information. The type of information that is required to transfer can be the parameter to decide the adapted Visual Cryptography approach. The purpose of information security or the organization or the person who is involving in the secure communication can decide the cryptographic level required to attain the secure communication. Some of the most used cryptographic approaches are explored here with algorithmic and result specification.

A) Random Key Visual Cryptography

As the name suggest, in such kind of cryptographic system, a random secret key is generated of fixed size. To estimate the randomize character to generate the crypto data, base value analysis is performed. Here table 1 is showing the relation between the key length and the base values.

Table 1 : Key Length to Base Value Conversion Table

Key Length	1	2	3	4	5	6	7	8
Base Value	17	16	15	14	13	12	11	10
Key Length	9	10	11	12	13	14	15	16
Base Value	9	8	7	6	5	4	3	2

Now from this table, the conversion of key-length txt data conversion can be performed. The steps involved in cryptographic process are given here under

Table 2: Cryptographic Algorithm

- Divide DataSet in N sub DataSets
- Now Dataset can be constructed from any K DataSets out of N
- Complete K-1 datasets can represents the dataset information
- Write kdatasets out of N
- A pixel *P is split into two sub pixels in each of the* two shares.
- If *P is white, then a coin toss is used to* randomly choose one of the first two rows in table defined above.
- Then the pixel *P is encrypted as two sub pixels* in each of the two shares, as determined by the chosen row in the table. Every pixel is encrypted using a new coin toss.
- If *P is black, then we get two black sub pixels* when we superimpose the two shares;
- If *P is white, then we get one black sub pixel* and one white sub pixel when we superimpose the two shares.

Thus, we could say that the reconstructed pixel (consisting of two sub pixels) has a grey level of 1 if *P is black, and a grey level of 1/2 if P is white.* There will be a 50% loss of contrast in the reconstructed image, but it should still be visible

In the case of visual cryptography, decryption is done by human visual system. It is already discussed that human visual system acts as an Ex-OR function. In the case of decryption, for computer generated program; Ex-OR function can be used.

Here the numbers of shares are taken as input from user. As the shares are created from the image taken as input in encryption algorithm, each share must be of equal height and width as the source image. Then bitwise Ex-OR operation is performed among pixels of the shares, and final pixel values are stored in an array. The decryption algorithm is as follows.

```
Algorithm(Img)
/*Img is the encrypted image taken as input for the decryption process*/
{
    1. For i=1 to Size(Image)
       {
    2. Px=GetPixel(Image(i))
       [Read the pixel from Image]
    3. Divide the Pixel in N sub blocks called Px1,Px2….PxN
    4. Process Each Pixel Sub-Block under binary value analysis
    5. If (Px>Threshold)
       {
    6. Set Px=Black
       }
       Else
       {
    7. Set Px=White
       }
```



```
    8.  If (Count(black)>Count(White))
        {
    9.  Generate the subimage to black
        }
        Else
        {
    10. Generate the subimage to White
        }
    11. Reconstruct the Result Pixel Image
    12. Return Image
}
```

IV. **RESULTS**

The presented work is defined in mat lab environment to perform visual cryptography. The work is analyzed under different vectors. The results obtained from the work are given here under

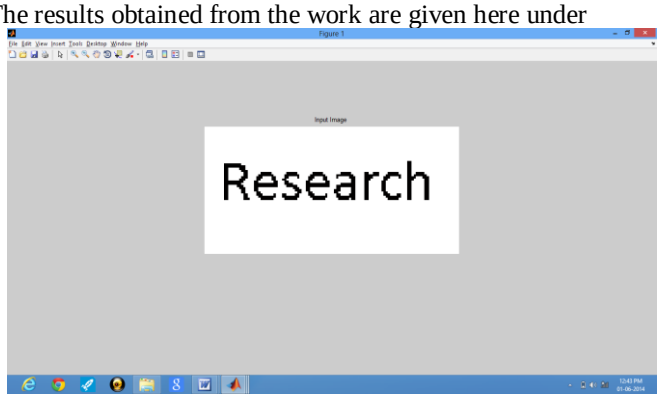

Figure 2 : Input Image

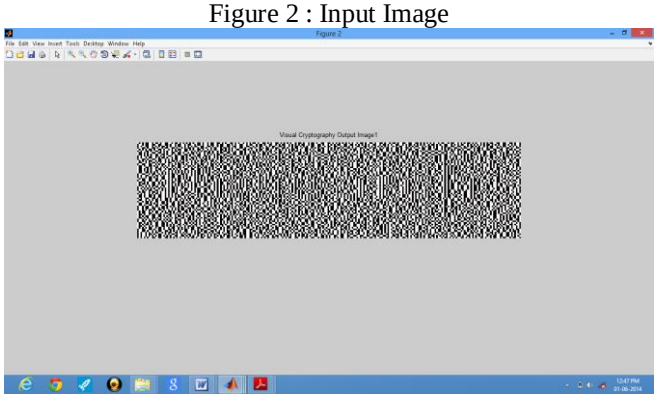

Figure 3: Result Image

Here figure 3 is showing the input image and figure 3 is showing the result encrypted image. The results shows that the work is effective to perform encryption.

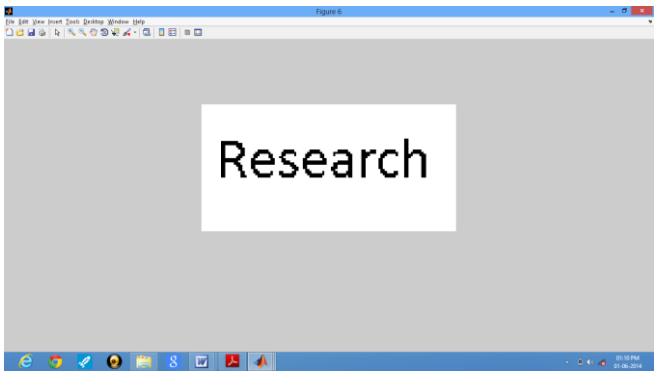

Figure 4: Recovered Image

Here figure 4 is showing the recovered image after the decryption process. The result shows the effective retrieval of actual image from encrypted.

V. CONCLUSIONS

One of the major aspects of information security is represented by cryptographic approaches. In this paper, the exploration to the available cryptographic approaches is defined. The paper has explored main cryptographic approaches called random key Visual Cryptography. The results obtained from the system shows that the presented work is effective enough to provide the effective throughput for encoding process.

REFERENCES

1. Louis J. Freeh, Keynote talk at International Visual Cryptography Institute, Sept. 1995. Available through http://www.fbi.gov/crypto.htm .
2. Liao H, Lee P, Chao Y, Chen C (2007). "A location-dependent data encryption approach for mobile information system", in the 9th International Conference on ADVANCED Communicate Technology 1: 625-628. Mundt TM (2005).
3. "Location dependent digital rights management system", in preceding the 10th IEEE symposition on computers and communication pp. 617-622.
4. Pandian PS (2008) "Wireless Sensor Network for Wearable Physiological Monitoring", J. Networks.
5. Richard W (2006). "Visual Cryptography and trust", information security tech-nical report. 11(6): 8 – 71.
6. GPP, 3G TS 35.201 "Specification of the MILENAGE Algorithm Set: An example algorithm set for the 3GPP authentication and key generation functions f1, f1*, f2, f3, f4, f5 and f5*.
7. Document 1: General" L.I. Millett, S.H. Holden, "Authentication and its privacy effects", IEEE Internet Computing, Nov. 2003.
8. Heikki Kaaranen, Ari Ahtiainen, Lauri Laitinen, Siamak Naghian, and Valtteri Niemi, UMTS Networks: Architecture, Mobility and Services, 2nd Edition, John Wiley & Sons, Ltd., 2005.
9. F. Zhang, W. Susilo, and Y. Mu, Identity-based partial message recovery signatures (or How to shorten ID- based signatures), In Proceedings of Financial Visual Cryptography- FC'05, LNCS 3570, pp.45-56, 2005.
10. M. Abe and T. Okamoto, A Signature Scheme with Message Recovery as Secure as Discrete Logarithm, In Proceedings of the International Conference on the Theory and Applications of Cryptology and Information Security, LNCS 1716, pp. 378-389, 1999.
11. C. Y. Chow, M. Mokbel, and X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based services," in *Proc. of the ACGIS*, 2006, pp. 247–256.
12. G. Ghinita, P. Kalnis, and S. Skiadopoulos, "PRIVE: Anonymous location-based queries in distributed mobile systems," in *Proc. of the 1st Int. Conference on World Wide Web (WWW)*, 2007, pp. 371–380.
13. B. Gedik and L. Liu, "Privacy in mobile systems: A personalized anonymization model," in *Proc. of ICDCS*, 2005, pp. 620–629.
14. M. Mokbel, C. Chow, and W. Aref, "The new casper: Query processing for location services without compromising privacy," in *Proc. of VLDB*, 2006, pp. 219–229.

