# A Hybrid Geometric Cryptography Approach to Enhance Information Security

Tanu
Department of Computer Science and Engineering, Sat Priya Group of Institutions, Rohtak, Haryana, India.

Rupali Malhotra
H.O.D in Computer Science Department, Sat Priya Group of Institutions, Rohtak, Haryana, India.

**Abstract – It is widely recognized and accepted that data security will play a crucial and critical role in modern times for businesses will be transacted over the Internet through e-commerce and m-commerce channels. To address these security concerns, various security protocols that are of symmetric-key and asymmetric-key type have been developed. In this paper, we present the hybrid cryptography approach with the specification of two geometrical shapes i.e. ellipse and the rectangle. Two geographical shapes are taken as the cover to place the information and the series of geometric transformation operations are defined to encode the information, which uses the properties of ellipse, rectangle and symmetric-key algorithm, the algorithm is based on 2-d geometry using property of ellipse and rectangle. The work includes hybrid geometric shapes and alternative transformation so that more information security will be achieved. Also the work includes dynamic generation of key; it will provide more robustness against information size.**

**Index Terms – Cryptography, Encryption, Decryption, Hybrid cryptography, Transformations.**

## 1. INTRODUCTION

A Hybrid Geometric Approach is a symmetric key cryptographic technique [1] [2] which is used to encrypt the data. This is a new process which uses the principles of Computer Graphics and properties of geometrical shapes in the encryption of data [3]. In our cryptography technique, some geographical shape is taken as the cover to place the information and the series of geometric transformation operations are defined to encode the information. This type of encryption includes hybrid geometric shapes and alternative transformation more information security will be achieved. The key is generated dynamically; it will provide more robustness against information size. The key is also not prefixed rather it gets generated during the process of encryption. Cryptography is the scheme that is used to encrypt a simple text. It hides the meaning of the message. Cryptography algorithms are the mathematical functions that are used for encryption and decryption. In cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers cannot read it, but that authorized parties can. In an encryption scheme, the message or information (referred to as plaintext) is encrypted using an encryption algorithm, turning it into an unreadable cipher text. This is usually done with the use of an encryption key, which specifies how the message is to be encoded. Any adversary that can see the cipher text should not be able to determine anything about the original message. An authorized party, however, is able to decode the cipher text using a decryption algorithm that usually requires a secret decryption key that adversaries do not have access to [4, 14]. Cryptography is of two types: one is symmetric cryptography and other is asymmetric cryptography [5, 15].

### 1.1. Symmetric Cryptography

Symmetric cryptography is the cryptosystem in which a single key or the same key is used to encrypt and decrypt the message. So the symmetric cryptography is also known as shared key or single key cryptography. A number of symmetric key encryption algorithms like DES, TRIPLE DES, AES, BLOWFISH have been developed to provide greater security affects.

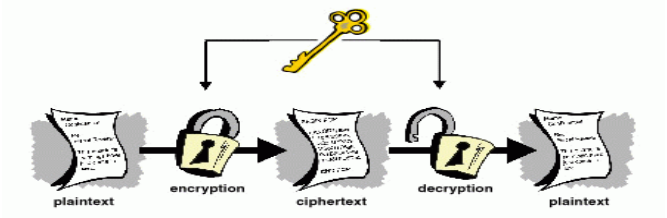


Figure 1: Symmetric Key Cryptography

### 1.2. Asymmetric Key Cryptography

Asymmetric key cryptography is also known as public key cryptography. It uses two different keys: - one public key and the other is private key. It is computationally hard to find the private key from the public key. Anyone can encrypt a message with the public key but not decrypt it. The person who has the private key can only decrypt the message. The sender encrypt the data using the receiver's public key and the receiver decrypt the data with its own key known as private key. There are a number of Asymmetric key encryption algorithms like RSA, ECC.

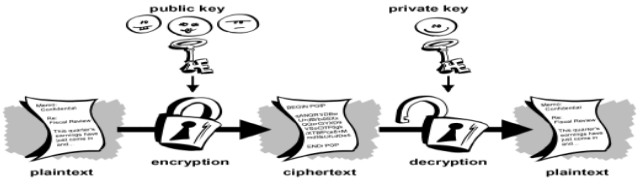


Figure 2: Asymmetric Key Cryptography

In this paper, the new approach for cryptography is presented to improve the security. The work is defined under I, use of geometrical shapes and apply transformations for reliable communication. In section II, the work defined by earlier researchers is discussed. In section III, the proposed research model is presented. In section IV, the results obtained from the work are presented. In section V, the conclusion of the work is presented.

## 2. RELATED WORK

There are several researchers of the different great minded person that leads the way toward the unbreakable secure system. . In this paper, some of the contribution of earlier researchers is discussed. Gurjinder Kaur performed a work, "Asymmetric Cryptography Based on Sphere." ACBS: Known parameter: - center of Sphere (Public Key). Key Generation: - using Distance method of Sphere we generate the pair of Public-Private Key. Elliptic curve cryptosystem provides an efficient alternative to other cryptosystems. Prerna Gaur performed a work "Geometry Based Symmetric Key Encryption Using Ellipse" implement a new approach for symmetric Encryption using the concept of Cartesian Plotting, ellipse generation and translation, rotation is introduced. Here the random plaintext bits are placed on ellipses and these ellipses are translated and rotated to obtain cipher text. Sony Kamara performed a work," Dynamic Searchable Symmetric Encryption". Searchable symmetric encryption (SSE) allows a client to encrypt its data in such a way that this data can still be searched. Author proposes the first SSE scheme to satisfy all the properties outlined above. Presented construction extends the inverted index approach (Curtmola et al., CCS 2006) in several non-trivial ways and introduces new techniques for the design of SSE. In addition, Author implement Presented scheme and conduct a performance evaluation, showing that Presented approach is highly efficient and ready for deployment [6]. Jaesung Yoo performed a work," A Method for Secure and Efficient Block Cipher using White-Box Cryptography". In this paper, Author mentioned White-Box AES proposed by Chow et al. and improve its low performance and key update problem. Author adopted composite mode using White-Box AES and Standard AES. Presented scheme shows almost same performance with Standard AES and provides dynamic key approach effect. Moreover, it has a CPA-secure property and can be constructed for CCA-secure scheme with Message Authentication Code [7]. Trisha Chatterjee performed a work," Symmetric key Cryptosystem using combined Cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm". In the present paper the authors have introduced a new combined cryptographic method called TTJSA In the present work, authors modified the standard Vernam Cipher Method for all characters (ASCII code 0-255) with randomized keypad, and have also introduced a feedback mechanism [8]. Joonsang Baek performed a work," Compact Identity-Based Encryption without Strong Symmetric Cipher". In this paper, as contributions to this line of research, Author construct hybrid identity-based encryption schemes which produce compact cipher texts while providing both efficiency and strong security without resorting to the strong length preserving symmetric cipher. Author provides security analysis of Presented schemes against chosen ciphertext attack under the well-known computational assumptions, in the random oracle model [9]. Bibhudendra Acharya performed a work," Image Encryption using Index based Chaotic Sequence, M Sequence and Gold Sequence". In this paper Author encrypted image using Index based chaotic sequence, M sequence and Gold sequence. The algorithm is experimented on the gray scale image. The Index based chaotic sequence algorithm permutes the image on the basis of index position of chaotic sequence. The process of permutation is based on storing the index position of the sequence in respected to their sorted value [10]. Ralf Kusters performed a work," Computational Soundness for Key Exchange Protocols with Symmetric Encryption". In this paper, Author show the first general computational soundness result for key exchange protocols with symmetric encryption, along the lines of a paper by Canetti and Herzog on protocols with public-key encryption [11]. Craig Gentry performed a work," Fully Homomorphic Encryption Using Ideal Lattices". Author propose a fully homomorphic encryption scheme – i.e., a scheme that allows one to evaluate circuits over encrypted data without being able to decrypt. Presented solution comes in three steps. Author describes a public key encryption scheme using ideal lattices that is almost boots trappable. The proposed scheme is simple and easy to be implemented for shadow images. Therefore, it can be used in many electronic business applications [12].Giuseppe Ateniese performed a work," Provably-Secure Time-Bound Hierarchical Key Assignment Schemes". In this paper Author design and analyze time-bound hierarchical key assignment schemes which are provably-secure and efficient. Author first considers the unconditionally secure setting and Author show a tight lower bound on the size of the private information distributed to each class. Author proposes two different constructions for time-bound hierarchical key assignment schemes [13].

## 3. PROPOSED MODEL

In this present work, new cryptographic approach is used to improve the chances of key prediction. In this cryptography approach, some geographical shape is taken as the cover to

place the information and the series of geometric transformation operations are defined to encode the information. The work is here defined as the hybrid cryptography approach with the specification of two shapes i.e. ellipse and the rectangle. These shapes will be placed in the geographical area alternatively and information will be stored on boundaries of the shapes in bit form. The transforming operations on these two shapes will be applied separately. For ellipse rotation and translation will be applied in series whereas for rectangle these operations will be applied in reverse order. Another major advantage of this proposed algorithm is its robustness against information size. It means, the area dimensions and shape size will be analyzed at initial stage based on the information size. The work will be about to improve the security. Here figure 3 has showed the cryptographic model defined in this work to perform the geometric cryptography. According to this cryptography model at first the input is taken in the textual form. This input is then analyzed under the geometric adaptation. The analysis on this input is performed. For this analysis, the text is converted to bit form. Based on this bit adaptive size is required to store the data in bit form. Now the required number of bits and relatively required size of canvas is identified. The area based split is here done to identify the number of possible shapes that can be drawn over the geographical area. From this analysis the actual key will be obtained to perform the cryptography.

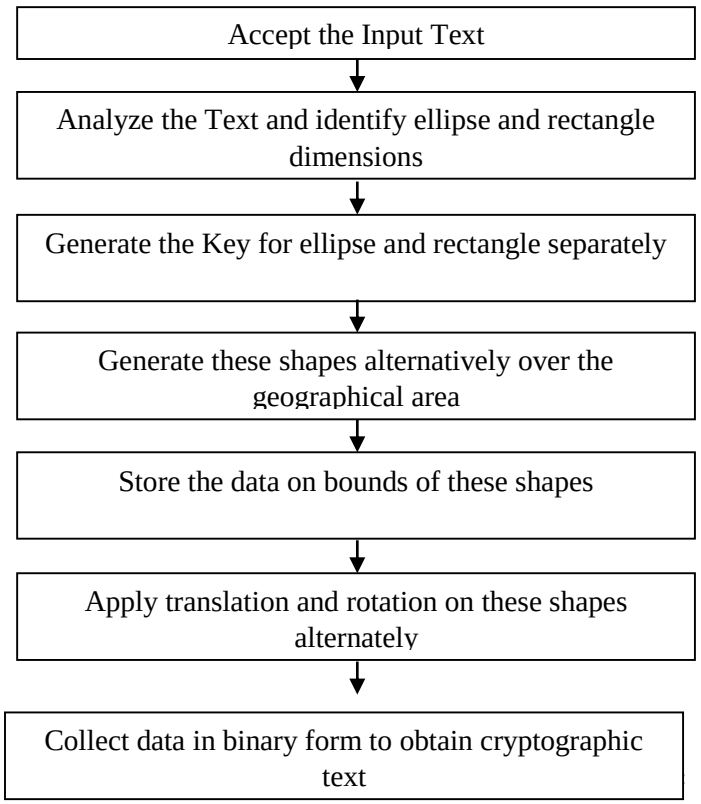


Figure 3: Flow of Work

Once the key is generated, the next work is to generate the shapes alternatively over the defined geographical area. This shape generation process is repeated till the complete geographical area is not got covered. Finally the bit adaptive model is applied to store the data at identified location. After collecting these bits, the actual cryptography is obtained. The flow of work is given in Figure 3.

The work is processed into two parts:

3.1. Input Text Processing

In this part, the text file is selected, this file contain the data to be encrypted. This processing includes the analyses for geometrical shapes and also performs key generation as per the parameters of ellipse and rectangle. The text file data converted into binary shape in order to store the data on the boundary required in next part of processing.

3.2. Geometric Area Processing

In this part, we generate ellipses and rectangles in hybrid manner using key generated in previous step then we record the data on the bound of these shapes. Now the encoding is performed. After encoding our information, we can get our original data by using decoding scheme in vice-versa manner.

The presented work model is here defined under the specification of the input text, key and the obtained algorithm. As the plain text is input, the analysis is here performed to generate the key. This dynamic key formation model has improved the strength of work.

Once the encoding is done, the data is transmitted and on the receiver side the decoding process is applied. The decoding is here done using the same key and the final normal text is obtained from the work. The key strength of this adapted model includes the alternate shape adaptive data storage. In this work, two shapes are considered called ellipse and the rectangle. These shapes are drawn on the geographical area in a sequence. Once the shape is drawn, the next work is to store the data on this location. The data is stored here in bit form. After obtaining the shape adaptive data storage, the next work is to perform the encoding. In this work geometric transformation is applied to perform the encoding. In this work two methods are applied to perform encoding. These methods are scaling the rotation algorithms. These algorithms are applied on each location of the stored data bit and the encoded data bits are obtained. Finally the data is retrieved and converted back to the secret form.

The work includes hybrid geometric shapes and alternative transformation more information security will be achieved. As the work includes dynamic generation of key, it will provide more robustness against information size. Thus the work is to define a hybrid cryptography approach using ellipse and rectangles, to analyze the cryptographic area dimensions dynamically based on information, to define the alternative

transformations for different geometric shapes, to analyze the work under efficiency and size vectors.

## 4. RESULTS

The analysis of this presented work is done in terms of time taken.

| Input Length | Encryption Time | Decryption Time |
|---|---|---|
| 100 | 7 | 6 |
| 200 | 13 | 11 |
| 300 | 25 | 20 |
| 400 | 32 | 25 |
| 500 | 38 | 31 |

Table 1: Analysis Result

The time adaptive analysis obtained from the work on encryption and decryption process is shown in table 1.

The results are here analyzed respective to different length inputs for encryption and decryption process. The results are shown in the form of graph:

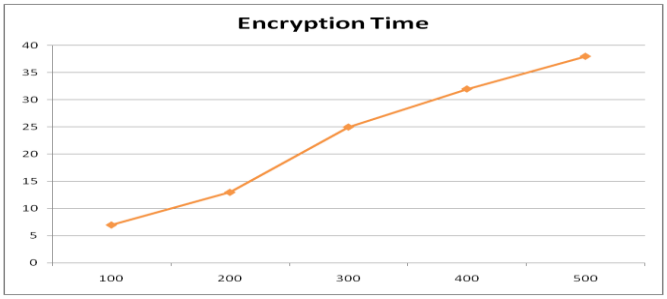


Figure 4: Encryption Time Analysis

Here Figure 4 is showing the time taken to encrypt the input text. Here x axis showing the size of input text and y axis shows the time in milliseconds.

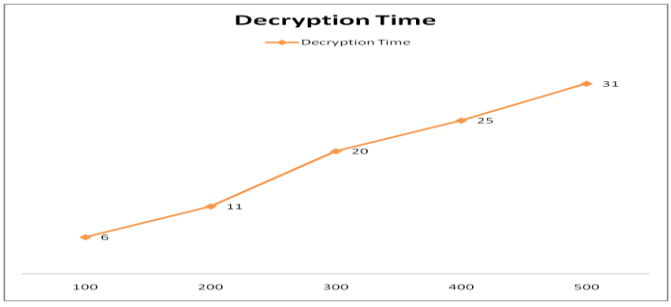


Figure 5: Decryption Time Analysis

Here Figure 5 is showing the time taken to decrypt the input text. Here x axis showing the size of encrypt text and y axis shows the time in milliseconds.

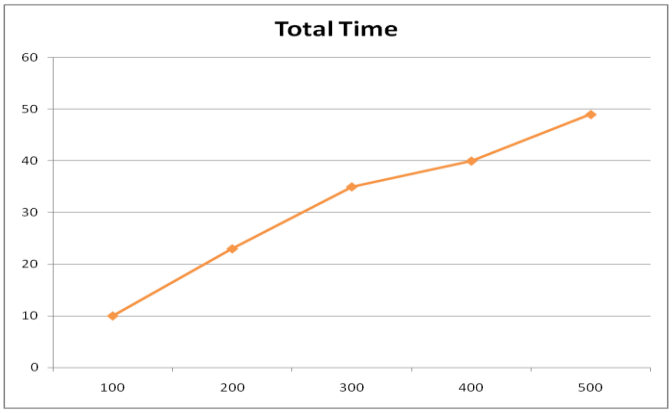


Figure 6: Total Time Analysis

Here Figure 6 is showing the time taken to encrypt and decrypt the input text. Here x axis showing the size of encrypt text and y axis shows the time in milliseconds.

## 5. CONCLUSION

In this present work, a dynamic key adaptive alternative shape based geometric cryptography model is presented. The work is defined as the dynamic and robust model so that the effective information security will be achieved. The presented work model is divided in number of associated stages. In first stage, the dynamic key is generated using message level analysis. The geographical area and the object features are obtained from the key. Based on this, in second stage, the alternate shapes are drawn as ellipse and rectangles. In third stage, the data is stored on these shapes in binary form. In next stage, the transformation is applied to perform data encoding. Finally on receiver side, the reverse operation is performed to perform data decoding. The work has been about to improve the security.

## REFERENCES

[1] William Stallings Cryptography and Network Security, 3rd Edition, Prentice-Hall Inc., 2005.
[2] Behrouz A. Forouzan, Data Communication and Networking, 4th Edition, Tata McGraw Hill Company, 2006.
[3] Kumar P.Ramesh, S.S.Dhenakaran, K.L.Sailaja, P.SaiKishoreVirtus "CHAKRA: A New Approach for Symmetric Key Encryption", IEEE, 978-1-4673-4804-1, 2012.
[4] Prerna Gaur, Dr.Paramjit Singh, "Geometry Based Symmetric Key Cryptography Using Ellipse" International Journal of Application or Innovation in Engineering & Management Volume 2, Issue 7, July 2013 ISSN 2319 – 4847.
[5] Gurjinder Kaur,Simarjit Singh, AnuGarg, "ACBS: Asymmetric Cryptography Based on SPHERE", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 3, March 2014 ISSN: 2277 128X.

[6] Seny Kamara," Dynamic Searchable Symmetric Encryption", CCS 12, October 16–18, 2012, Raleigh, North Carolina, USA. ACM 978-1-4503-1651-4/12/10 (pp 965-976).
[7] Jaesung Yoo," A Method for Secure and Efficient Block Cipher using White-Box Cryptography", ICUIMC'12, February 20–22, 2012, Kuala Lumpur, Malaysia. ACM 978-1-4503-1172-4.
[8] Trisha Chatterjee," Symmetric key Cryptosystem using combined Cryptographic algorithms - Generalized modified Vernam Cipher method, MSA method and NJJSAA method: TTJSA algorithm", 978-1-4673-0125-1@ 2011 IEEE (pp 1179).
[9] Joonsang Baek," Compact Identity-Based Encryption without Strong Symmetric Cipher", ASIACCS '11, March 22–24, 2011, Hong Kong, China. ACM 978-1-4503-0564-8/11/03 (pp 61-70).
[10] Bibhudendra Acharya," Image Encryption using Index based Chaotic Sequence, M Sequence and Gold Sequence", ICCCS11, February 12–14, 2011, Rourkela, Odisha, India. ACM 978-1-4503-0464-1/11/02 (pp 541-544).
[11] Ralf Kusters," Computational Soundness for Key Exchange Protocols with Symmetric Encryption", CCS'09, November 9–13, 2009, Chicago, Illinois, USA.ACM 978-1-60558-352-5/09/11 (pp 91-100).
[12] Craig Gentry," Fully Homomorphic Encryption Using Ideal Lattices", STOC'09, May 31–June 2, 2009, Bethesda, Maryland, USA. ACM 978-1-60558-506-2/09/05 (pp 169-178).
[13] Giuseppe Ateniese," Provably-Secure Time-Bound Hierarchical Key Assignment Schemes", CCS'06, October 30–November 3, 2006, Alexandria, Virginia, USA, ACM 1-59593-518-5/06/0010 (pp 288-297).
[14] Amit Jain, Avinash Panwar, Divya Bhatnagar, "Design and Develop an Approach for Integrating Compression and Encryption on Textual Data", International Journal of Computer Networks and Applications (IJCNA), Volume 2, Issue 3, May – June (2015).
[15] R. Bhagavath Nishanth, Dr. B. Ramakrishnan, M. Selvi, "Improved Signcryption Algorithm for Information Security in Networks", International Journal of Computer Networks and Applications (IJCNA), Volume 2, Issue 3, May – June (2015).