Secure and efficient application of MANET using RSA using Vedic method combine with Visual cryptography and Identity based cryptography technique

Mohit Singanjude, Prof. R. Dalvi

Department of Computer Engineering,
Marathwada Mitra Mandal's College of Engineering, Pune Savitribai Phule Pune University, India.

***Abstract*—Security and fast transmission of data is very important part of military devices. Propose technique present the secure, efficient and fast way to send images by using the Identity Based Cryptography and Visual Cryptography. In this application Identity Based Cryptography is used with Visual cryptography. In Identity based cryptography the RSA Cryptosystem is used to generate public and private key by using Ancient Indian Mathematics for fast mathematical calculation. RSA is the safest and standard algorithm. Implementation of it by using the Vedic multiplication is very efficient in term of area, speed as compared to its modern mathematics implementations. The regenerations of public and private key are adopted to make the system more secure from various attacks.**

Keywords*— *RSA Cryptosystem, MANET, Vedic Mathematics, Modular Multiplication, Identity Based Cryptography, Visual Cryptography.

I. INTRODUCTION

Now a day's data security is very important part of military devices. Also, it needs to be work fast for sending and receiving secure data/images. Here the proposed technique presents the secured, efficient and fast way to send images by using the Identity Based Cryptography and Visual Cryptography. This technique can be specially used in MANET for the military surveillance. Here we use the Visual Cryptographic technique, due to its simplicity and efficiency makes it the appropriate choice for sending/receiving images and finds use in transmitting encrypted images. In the proposed technique the private/public key pair is used to make system more secure. Identity based cryptographic technique represents a system having a solitary base station with numerous mobile nodes which is identical to that of (MANET) Mobile Ad hoc Net-work. The steps of Identity based cryptography are adopted to set up the system and hence for encryption and decryption of data.

The Visual Cryptography was pioneered by Moni Naor and Adi Shamir in 1994. They come up with a visual secret sharing scheme, where an image is divided or broken up into number shares so that only someone with all n shares could decrypt the image, while someone with any n-1 shares can reveal no information about the original image. Each share is printed on a separate transparency and decryption is performed by overlaying the shares when all numbers of shares are overlaid, the original image gets appeared. The Visual Cryptographic is one of the new techniques which provided information security and uses the simple algorithm unlike the complex one used in the other traditional cryptography. This allows visual information like pictures to be encrypted in such a way that their decryption can be performed by human visual system without any complex computation or algorithms.

Identity-based cryptography use of user identity attributes, such as email addresses or phone numbers instead of digital certificates, for encryption and signature verification. This feature significantly reduces the complexity of a cryptography system by eliminating the need for generating and managing user's certificates. It makes much easier to provide cryptography to the unprepared users, since messages must be encrypted for users before they interact with any system components. Before secure communications can take place, both sender and receiver must generate encryption and signature key pairs, submit certificate requests along with proof of identity to a (CA) Certificate Authority, and receive CA signed certificates, which they can use it to authenticate one another and exchange encrypted messages with each other.

The RSA algorithm was publicly described in 1977; the letters RSA are the initials of their surnames (RivestShamirAdleman). RSA is asymmetric key encryption technique. It is widely used and most versatile public key algorithm today. RSA is mostly depending on the modular exponentiation of long integers. Regenerations of public and private keys of the complete system take place ensuring more effective data security. Therefore, fast modular multiplication becomes the key to real-time encryption/decryption since a high throughput is needed in data communication. Vedic Mathematics is based on 16 sutras dealing with mathematics related to arithmetic, algebra, and geometry. Application of the Sutras improves the computational skills of the learners in a wide area of problems, ensuring both speed and accuracy, strictly based on rational and logical reasoning. Vedic method is direct and extraordinary for their efficiency and simplicity for mathematical calculations.

To improve the security and speed of the transmit image to the destination with RSA encryption and decryption. Using Ancient Indian Vedic mathematics, the speed of RSA algorithm execution can increase. The Vedic is well known for fast calculation. System should function normally even if any military personnel have been captured that is additional requirement.

Our work proposes a system which will overcome the limitation of time required to generate the public private key.

II. LITERATURE REVIEW

Secure and efficient application of MANET using Identity Based cryptography combined with Visual cryptography technique [2], The (MANET) Mobile Ad hoc Network is useful application in military purposes as mobility is very important requirement in border surveillance. Also, the robustness of MANETs to function even in unknown terrain justifies its application as military

devices. Visual Cryptographic technique is uses due to its simplicity and efficiency makes it the appropriate choice for sending and receiving the images and finds use in transmitting encrypted images to and for base station from border military forces. Instead of using only private key generators, both public and private key pairs are getting to make the system more secure.

A Survey on Visual Cryptography Techniques and their Applications [5], Visual cryptography is a cryptographic technique which allows visual information to be encrypted in the way that decryption becomes a mechanical operation. Visual Cryptography utilizes two transparent images. One image contains random or noisy pixels and the other image contains the secret data. It is almost impossible to retrieve the secret information from encrypted images. Both transparent images and layers are required to reveal the information. Secure Transaction System Using ID Based Cryptography [6], present a modified model to authenticate clients for online transaction transactions through utilizing Identity-Based Cryptography techniques in conjunction with the one-time ID concept for the purpose of increasing security. The Identity-based public key encryption facilitates easy introduction of public key cryptography which allows an entity's public key to be derived from an arbitrary id value, such as name or email address or birth date. The main practical benefit of identity-based cryptography is in greatly reducing the need for, and reliance on, public key certificates.

VLSI Implementation of High-Performance RSA Algorithm Using Vedic Mathematics [1], presented Vedic Karatsuba multiplication and Vedic Booth Algorithm is superior over a conventional Karatsuba multiplier in terms of speed and the scalability of the multipliers is also seems to be good. There are standard techniques for providing privacy and security in data networks include with the encryption and decryption algorithms such as (AES) Advanced Encryption System (private-key) and RSA (public-key). RSA is one of the safest and standard algorithms, based on public-key, for providing security in the networks. Implementation of RSA Cryptosystem by Using Ancient Indian Vedic mathematics [3], in implementation of the RSA encryption/decryption algorithm using with help of Ancient Indian Vedic Mathematics algorithm that have been modified to improve the performance. RSA circuitry implemented by using the Vedic multiplication that is very efficient in terms of area, speed as compared to its implementation using conventional multiplication. The most significant aspect is the development of division architecture based on Ancient Indian Vedic Mathematics and embedding it in RSA encryption and decryption circuitry for improved the efficiency.

III. PROPOSED SYSTEM

Figure 1 show the architecture of proposed system and description of the system is as follows.

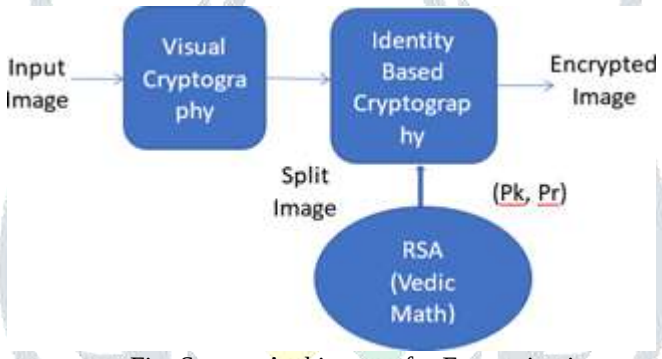


Fig: System Architecture for Encryption images

The proposed system encrypts the image for secure transmission. The input image is provided by the sender. The input image is split into the shares with the help of visual cryptography. That divides the image into N shares. On overlapped image is encrypted using identity cryptosystem. The identity-based cryptography generates private and public key with the help of RSA algorithm. The RSA algorithm performs the calculation with the help of Vedic mathematics to generate the private and public key. Thus, the output of image is encrypted image.

Input: The input image will be provided by the sender to encrypt. The dummy image H is input, S is binary secret image with S1*S2 pixel, Public Key Pk.

Visual Cryptography: The original image is split into two or more shares. All the shares are requires decrypting the information. Each of the pixels is sub divided into four sub pixels. The shares of image are provided to the Identity Based cryptography system to generate the public and private key.

Identity Based Cryptography: The shares of images are provided by the Visual cryptography techniques. The Identity Based cryptography provides the public key to the user with the help of RSA method.

RSA: Each node has its public and private key (Pk, Pr) in PKG. For making work of system simpler and faster, we use the RSA pairing for encryption and decryption. To generate the public and private key the Vedic mathematics is used for faster calculation. The generated public and private key provided to the Identity Based Cryptosystem.

Expected Output: The encrypted secrete image of size S1*S2 pixels, each of which is composed of 4 subpixels.

IV. PROPOSED ALGORITHM

Visual Cryptography

Step 1: In encryption phase it takes secrete image, dummy image and public key as an input. The mean Xm of pixel value of dummy image is calculated.

Step 2: The random number lists is generated [1,2, 3...H*W] where H and W is Height and Width of image. Using random numbers, the sample of n=30 pixels are selected from list.
Step 3: The mean Xs is calculated of a sampled pixel.
Step 4: By applying rules, pixels are encrypted each of which is composed of four subpixels. The rules basically use Xm and Xs to divide the pixel.
Step 5: These steps are repeated until all pixel of secret image is picked.
Step 6: Stop

In this algorithm the user has provide the image as input to the Visual cryptography. For the encryption of image, it takes secrete image, and dummy image also the public key as input value. It calculates the mean value of the dummy image. The random number of lists is generated Height and Width of the image. Using the random numbers, the sample of n=30 pixel is selected from the list. The mean value Xs is calculated of a sampled pixel. By applying rules, pixels are encrypted each of which is composed of four subpixels. The rule basically uses Xm (pixel values of dummy image) and Xs (sampled pixels) to divide the pixel of image. All steps are repeated until the pixels of secret image are picked.

Identity Based Cryptography

Setup: a secret image s and a P master public key by using a random numbers generator. Then it publishes P and s.
Key Generation: takes a master secret key msk, a public parameter PP and an identity ID, generate private key for ID Encrypt: Take as input parameters, ID, M. It returns ciphertext c.
C=Encrypt (parameter, ID, M)
Decrypt: Take input parameter, c, and private key d. It returns original massage.
M= Decrypt (parameter, c, d)

In the Identity Based Cryptography that perform the operation to provide the public and private keys. In this setup the secret image and the master public key provide to the user. In key generation the output is a master public key mpk and master secret key msk. This algorithm is executed once by the authority when setting up the system. In the encryption phase it encrypts the image by using ID, as a public key. When receiver has received the image, he contact to the key server. The key server contact to a directory or other external authentication source for authenticate receiver identity and establish any other policy elements. After it authenticating receiver, the key server then returns its private key, with which receiver can decrypt the secret message. This private key can be used to decrypt all the future messages received by receiver.

Objectives and Challenges

At border military patrolling personnel needs to send some urgent images to their control room. In previous method of RSA time taken to execute algorithm is high. To overcome that problem, we use the Vedic mathematics. This reduces the time of execution by minimizing shift operations and performing multiplication in parallel. To implement the Identity Based Cryptography for encryption/decryption use RSA algorithm. RSA is the best algorithm for generating public/private key. The Vedic mathematics is well known for fast calculation as compare modern mathematics. So, it will provide fast encryption/decryption to transmit image secure and efficient.

Project Scope

The scope of the project is to increase the speed of encryption and decryption. The system mainly used in the high secured communication system for fast transmission of image. The Vedic mathematics is well known for fast calculation as compare modern mathematics. RSA is the best algorithm for generating public/private key.

Problem Statement

The military devices need to be fast and secure transmission of image from user to base station. To improves the security and speed of the sending images to the destination with RSA encryption and decryption. Using Ancient Indian Vedic mathematics, the speed of RSA algorithm execution can increase. Additional requirement is that system should function normally, even if any military personnel have been captured.

V. MATHEMATICAL MODEL

Consider a system M to divided each pixel of secrete image.

$$M = \{S0, X, \delta, O, Se\}$$

where,
S0 is Start State (Pixel 0),
X is input {0/1},
δ is transition function {Xm, Xs}
O is a, b; a and b are split pixels.
Se is end state (pixel H × W)

The identity-based cryptography is used to encrypt the split image. This algorithm takes the (M) Message, (P) the System Parameters, (Pk) Public Key and (C) Outputs the encrypted message.

Input Parameters to Encryption: System Parameters: St, P1t, P2t, the P1t, P2t are large prime numbers, St Multiplication of both prime numbers.

Input parameters to Decryption: The Encrypted message(C), Private Key (Sk) and Outputs the original message(M).

Encryption Key: (Et, St) Decryption Key: (Dt, St)

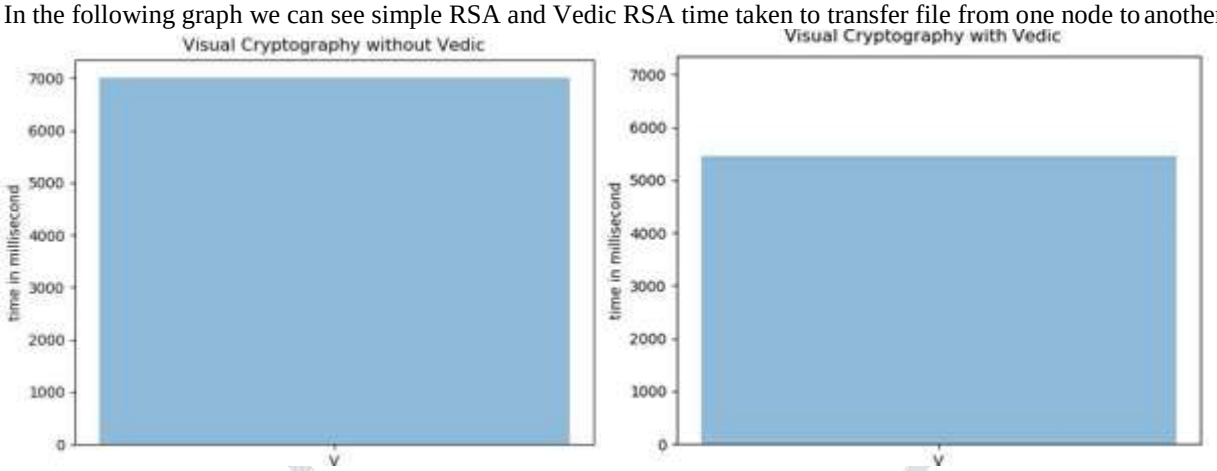
VI. EXPERIMENTAL SETUP AND EVALUATION

To create the MANET, we will connect three or more devices in wi-fi connection by creating HotSpot for communicate with each other in network. One device will act as Base station and other devices are nodes which will connect to base station. Image or Data will be transmitted from device to device. Base station will provide public and private key to connected devices for securely transmission of the data in network system

The proposed system result will be evaluated by comparing the processing time of existing system with the processing time of proposed system. The processing time includes the time of RSA encryption and the time requires generating public key and private key for each device in network.

VII. RESULT

In the following graph we can see simple RSA and Vedic RSA time taken to transfer file from one node to another node.



Hence this method will improve the performance of RSA cryptography.

VIII. CONCLUSION

We proposed this paper to increase the speed of encryption and decryption of image or data. The Identity Based Cryptography uses the private and public key for each device Id in a MANET. The PKG generates this key for each device- id and stores at base station only. These keys are refreshed by PKG at base station, so by adding RSA implementation with Vedic mathematics it improves the overall performance of the system.

IX. REFERENCES

[1] S. Kumaravel, Ramalatha Marimuthu, VLSI Implementation of High- Performance RSA Algorithm Using Vedic Mathematics, International Conference on Computational Intelligence and Multimedia Applications 2007.

[2] R. K. Sharma, Neeraj Kishore, Parijat Das, Secure and efficient application of MANET using Identity Based cryptography combined with Visual cryptography technique, International Journal of Engineering and Computer Science ISSN:2319-7242 Volume 3 Issue 2 February,2014.

[3] Shahina M. Salim, Sonal A. Lakhotiya, Implementation of RSA Cryptosystem Using Ancient Indian Vedic mathematics, International Journal of Science and Research (IJSR) ISSN (Online): 2319-7064 Index Copernicus Value (2013)

[4] S. P. Pohokar, R. S. Sisal, K. M. Gaikwad, M. M. Patil, Rushikesh Borse, Design and Implementation of 16 x 16 Multiplier Using Vedic Mathematics, 2015 International Conference on Industrial Instrumentation and Control (ICIC) College of Engineering Pune,
India. May 28-30, 2010

[5] Ms. Bhawna Shrivas, Prof. Shweta Yadav," A Survey on Visual Cryptography Techniques and their Applications", hawna Shrivas et al,
/ (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (2), 2015, 1076-1079

[6] Jaydipsinh B. Jadeja, Harikrishna Jethva, Bhadreshsinh G. Gohil" Secure Transaction System Using ID Based Cryptography", Jaydipsinh
B. Jadeja et al, International Journal of Computer Science and Mobile Computing, Vol.2 Issue. 12, December-

[7] G. Ganesh Kumar, V. Charishma Design of High-Speed Vedic Multiplier using Vedic Mathematics Techniques, International Journal of Scientific and Research Publications, Volume 2, Issue 3, March 2012.

[8] Sriraman, L. Dept. of Electron. Commun. Eng., Oxford Eng. Coll., Trichy, India; Kumar, K.S.; Prabakar, T. N," Design and FPGA implementation of binary squarer using Vedic mathematics" IEEE Trans. Ind. Electron., July 2013