Research Journal of Information Technology 4(2): 88-92, 2012
ISSN: 2041-3114

Submitted: April 18, 2012 Accepted: May 23, 2012 Published: June 30, 2012

A Novel Cryptographic Key Generation Method Using Image Features

B. Santhi, K.S. Ravichandran, A.P. Arun and L. Chakkarapani
Department of ICT, School of Computing, SASTRA University, Thanjavur

Abstract: Several methods in steganography and cryptography have been proposed for secured communication. But many compromises are there in them. Steganography which deals with security using multimedia has a very big disadvantage of increase in the information size. Cryptography which deals with encryption using the keys generated by various algorithms has the disadvantage of difficulty in remembering the key which can be easily cracked. The main objective of this study is to increase the security in communication by encrypting the information with the key generated by using an image. This study proposes a novel algorithm for key generation using image features. It is a reliable and flexible method of key generation for information security. In this method the user need not remember the keys during encryption and decryption. This study uses the Gray Level Co-occurrence matrix of an image to extract the Gray Level Co-occurrence properties of the image. A 56-bit sub-key is generated from the extracted Gray Level Co-occurrence properties. Then the key for encryption and decryption is generated using the sub-key generated from the image. This proposed method is easy to implement. The key strength is much better than others.

Keywords: Decryption, encryption, gray level co-occurrence matrix, gray level co-occurrence properties, image features, information security, sub-key

INTRODUCTION

We cannot think about a world without communication. With faster growth of internet, communication has become very easy. There are many methods in cryptography and steganography for providing secured communication. In secure communication, key generation phase has many challenges and this problem can be solved if the sender and the receiver share the key in any other form or if they generate the keys readily during the encryption and decryption separately. Thus, the concept of generating the key from an image came to the role. It should be very flexible, at the same time there should not be any compromises in the key strength and information security. The main objective of this study is to create novel algorithm for secure communication with image features. The proposed algorithm is simple to implement and user friendly algorithm. This algorithm flow is depicted for sender and receiver respectively in Fig. 1 and 2. Further, the algorithm is split up into five phases that is given in Table 1. This study uses images which are taken from the Google search engine and features have been computed from those images.

LITERATURE REVIEW

Lifang *et al*. (2010), have proposed a novel method for key generation using face features. Ogiela and Ogiela (2011), have developed a method for key generation using the biometrics (from images). Thekey generation from face features has a limitation that the process of key generation in this study is complex and lengthy process, even though it is secured. Kai-zhi *et al*. (2011), have discussed about a method for extracting the f eatures from the co-occurrence matrix. Fengxi *et al*. (2010), have proposed a method for feature selection using principal component analysis. Tanmay *et al*. (2011), have developed a method for key generation based on sessions.In general the key generated by the cryptographic methods must be remembered and they can be easily cracked.

MATERIALS AND METHODS

GLCM: GLCM calculates the number of occurrences in an image which is in a scaled version. It is also known as gray level spatial dependence matrix. The Gray level co-occurrence matrix is used to find the gray level co-occurrence properties of the image.

Feature extraction: It is a special form of dimensionality reduction. It is the process of transforming the input data which is redundant and very large to be processed into a reduced set of features. This set of features is known as the feature vector. This process of this trans formation is known as feature

Corresponding Author: B. Santhi, Department of ICT, School of Computing, SASTRA University, Thanjavur

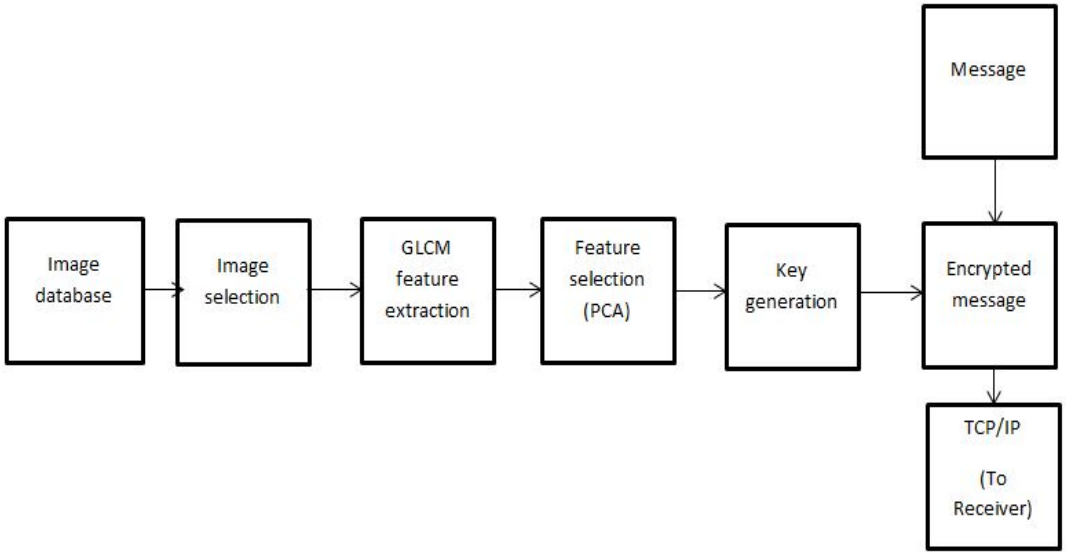

Fig. 1: Sender side block diagram

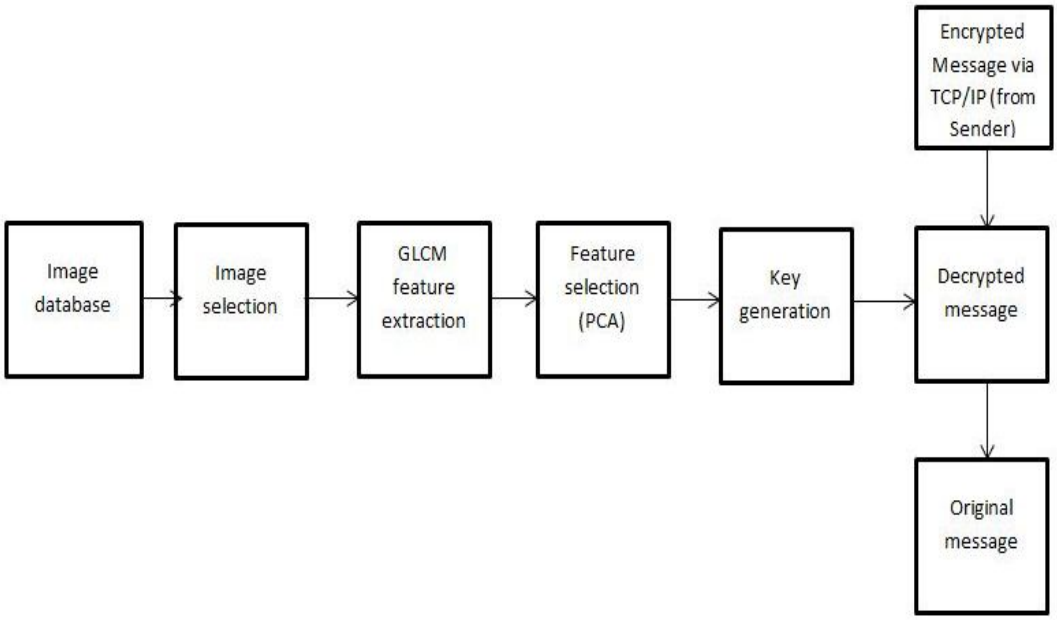

Fig. 2: Receiver side block diagram

Table 1: Phases in the entire process

Phases	Process
Phase 1	Database creation
Phase 2	Key generation
Phase 3	Encryption
Phase 4	Secure communication
Phase 5	Decryption

extraction. In this process we extract 23 features from the image.

Principal component analysis: Principal component analysis is a multivariate analysis based on eigen values and eigen vectors. It deals with multidimensional data. It is a linear transformation which transforms the data from its co-ordinate system to a new co-ordinate system. The features extracted from the image are given as input for Principal component analysis to select higher rank features.

Feature selection: Feature selection is dimensionality reduction of the given data. It involves the selection of the features with higher rank (priority). The features extracted from the gray level co-occurrence matrix are given as input for Principal component analysis and feature selection is done.

Key: A cryptographic key is the information generated to encrypt and decrypt the message. At the encryption side the cipher text is generated from the plain text by using the key. At the decryption side the exact reverse is done to get back the plain text.

TCP/IP: Transmission control protocol is a protocol used along with the internet protocol to send the data in the form of message units between two computers over the internet. Transmission control protocol will track the individual units of data and the Internet protocol will handle the actual delivery of data.

PROPOSED ALGORITHM

This study implemented the key generation as 1 key/session (1 session is 1 h). This can be enhanced by taking the minutes and seconds into account.

Phase 1: Database creation: Create the image database which is to be used for the key generation. Algorithm uses one image at a time. Implement the key generation algorithm.

In our experimental setup both the sender and receiver has used 24 images (1 image for an h). Both the sender and receiver should use same image databases and an image with both users should be of same name. This study has implemented this idea with 24 images but this can be extended even up to milliseconds.

Phase 2: Key generation:

Step 01: The gray level co-occurrence matrix of an image (2D image) is calculated;
Step 02: The gray level co-occurrence properties of the gray level co-occurrence matrix of the image is calculated;
Step 03: Retrieve the best four properties of the available gray level co-occurrence properties.
Step 04: Round all the property values and find the sum of all the properties;
Step 05: Convert the property values which are in decimal to binary values;
Step 06: Find the maximum and minimum length of the converted binary values;
Step 07: Append required number of bits to left of the binary values to get the maximum length.
Step 08: Compare all the binary bit positions whether all the properties have same value (either 1 or 0);
Step 09: Store the matching positions in an array.
Step 10: Find the sum of all the matching positions and their average;
Step 11: Sum all the property values (decimal)
Step 12: Round the sum value to get a four digit value.
Step 13: Perform binary division to the sum;
Step 14: Assign the characters for each digit of the quotient. (eg., if 0 = 'A', 1 = 'B',…, 25 = 'Z') and store them in an array. (We can modify this step by assigning the characters differently.)
Step 15: Repeat the last two steps until we get quotient 1;
Step 16: Reverse the character array and store it in another array.
Step 17: Concatenate the two arrays and form a new array;
Step 18: Choose the first 56 bits or the last 56 bits of the new character array and discard the remaining characters;
Step 19: Find the sum of the ASCII values of all the characters;
Step 20: Divide the 4 digits sum into 2 digits;
Step 21: If the 2 digits are greater than 26, sum the 2 digits and take it as one value;
Step 22: Perform the step 21 for the other 2 digit number;
Step 23: Finally, the key for encryption has been generated;

Phase 3: Encryption:

Step 1: Input the string to be encrypted and store it in a variable;

Step 2: Input the keys generated (left division and right division) from the images.

Step 3: Get the size of the string.

Step 4: Assign a flag = 0;

Step 5: If the position is even, then add the left division value with the variable. Else, add the right division value with the variable;

Step 6: If the flag is even, assign upper case character and add the character with the output of the previous addition. Else, assign lower case character and add the character with the output of the previous addition;

Step 7: Perform this operation for the entire string and store the encrypted text in the variable.

Step 8: Print the encrypted string;

Phase 4: Secure communication:

Step 1: The encrypted string is chosen;

Step 2: The Internet Protocol address of the receiver is chosen:

Step 3: The port number for the communication is chosen.

Step 4: The message is sent to the receiver by the sender using TCP/IP;

Step 5: The receiver receives the encrypted message.

Step 6: The receiver reads the message in the file and stores it in the variable for decryption;

Phase 5: Decryption:

Step 1: Input the string to be decrypted and store it in a variable;

Step 2: Input the keys generated (left division and right division) from the images;

Step 3: Get the size of the string;

Step 4: Assign a flag = 0;

Step 5: If the position is even, then subtract the left division value with the variable. Else, subtract the right division value with the variable;

Step 6: If the flag is even, assign upper case character and subtract the character with the output of the previous subtraction. Else, assign lower case character and subtract the character with the output of the previous subtraction;

Step 7: Perform this operation for the entire string and store the decrypted text in the variable;

Step 8: Print the decrypted string.

Table 2: Feature selection from principal component analysis

Image	Contrast	Correlation	Energy	Homogeneity
jpg	0.0845	0.9821	0.2263	0.9648
jpg	0.0756	0.9657	0.2565	0.9660
jpg	0.0960	0.9724	0.2262	0.9553
pg	0.2412	0.9497	0.1175	0.9013
jpg	0.1634	0.9616	0.1519	0.9343

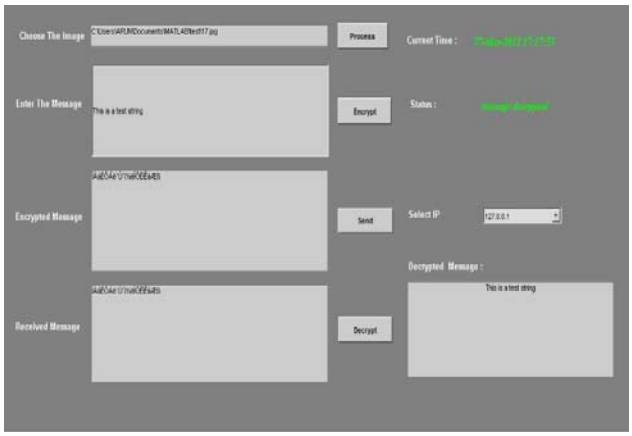

Fig. 3: Sender and receiver window

Fig. 4: Key generation window

EXPERIMENTAL RESULTS

The implementation of this key generation is done with 24 images for experimental purpose (1 image for an h). Both the sender and receiver should use same

images and an image with both users should be of same name. We have implemented this idea with 24 images but this can be extended even up to milliseconds. There are 22 features in an image. They are extracted from the Gray level co-occurrence matrix. They are given as input to the Principal component analysis for selecting the most dominant (top 4) features among them. In the below table the dominant features of the images and their values are specified. The images are named as 1, 2, …, 24 to specify the hours in a day. For example, if the time is 2 h (24 h format) then the image '2.jpg' will be chosen for key generation for encrypting the message. Thus, the key is generated from the image.

Using GLCM concept, Features are computed for images in available database.

Sample five images and its corresponding features are tabulated in Table 2. Based on this features and steps in phase 2 generates key for the secure communication. This is illustrated in Fig. 3. The encryption and decryption part of sender and receiver side is shown in Fig. 4 The image above is the graphical user interface of the sender and receiver window for the experiment.

The image above is the graphical user interface of the key generation window for the experiment.

CONCLUSION

The experimental results conclude that this method is more secured than traditional cryptographic processes and steganography. The process has an advantage of key generation based on sessions. This process is more flexible that any image can be used for key generation as the key generation is directly based on the image properties. In future, frequency domain image features may be used for key generation phase.

REFERENCES

Fengxi, S., G. Zhongwei and M. Dayong, 2010. Feature Selection Using Principal Component Analysis. ICSEM, 1: 27-30.

Kai-zhi, Y., C. Ying-lei and J. Liu, 2011. A method for extracting the text feature of SAR image based on co-occurrence matrix. 2011 4th International Congress on Image and Signal Processing (CISP), Telecommun. Eng. Inst., Air Force Eng. Univ., Xi'an, China, 4: 2038-2043.

Lifang, W., L. Xingsheng, Y. Songlong and X. Peng, 2010. A novel key generation cryptosystem based on face features. 2010 IEEE 10th International Conference on Signal Processing, 24-28 Oct. 2010, Sch. of Electron. Inf. Control Eng., Beijing Univ. Technol., Beijing, China, pp: 1675-1678.

Ogiela, M.R. and L. Ogiela, 2011. Image based crypto-biometric key generation. 2011 Third International Conference on Intelligent Networking and Collaborative Systems (INCoS), AGH Univ. Sci. Technol., Krakow, Poland, pp: 673-678.

Tanmay, B., H. Sirshendu, M. Ayan and S.R. Bhadra Chaudhuri, 2011. A novel data encryption technique by genetic crossover of robust biometric key and session based password. Int. J. Network Secur. Appl. (IJNSA), 3(2): 111-120, DOI: 10.5121/ijnsa.2011.3209.