International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 11 Issue 6 –NOVEMBER 2014.

Hiding Of Encrypted Information Using Stochastic Diffusion

Manibharathi. B[1], Rizvana.M[2] , and Prof Srinivasan. R[3]

[1]*M.Tech (IT) Student, Department of IT, PSV College of Engg & Tech, Krishnagiri, TN. India*

[2]*Assistant Professor, Department of IT, PSV College of Engg & Tech, Krishnagiri, TN, India*

[3]*Head of Department , Department of IT, PSV College of Engg & Tech, Krishnagiri, TN, India*

Abstract— Image authentication is the most famous technology in today's era which mainly provides security by the use of images. For this image is firstly encrypted by using some techniques. There are so many image authentication algorithms had proposed before but many of them are having disadvantages. To overcome this limitation we have proposed an image authentication by using the Stochastic Diffusion. In this method we are going to encrypt the digital image with the application of least significant bit. We have introduced new methods like watermarking algorithm for hiding image in single binaries host image. We have also used data hiding and randomized data methods for better image encryption and decryption. We are doing the cryptographic process on color images into 24 bit host hiding image.

Keywords: Encrypted Information Hiding; Stochastic Diffusion; Hidden Codes; watermarking algorithm.

I. INTRODUCTION

Digital image brought new issues in the computer science technology. Digital image has been adopted because their ease of processing, manipulation and storing is simpler and effective. The image authentication technique avoids malicious attacks while transmission of image over network. The image is being identified by using the watermarks present in the image. Few years ago the images are only known as a photographic proof. But now in early days image is use for many purposes, due to properties extensive of digital image. Basically image is a set of pixels arrange in (x, y) dimensions. Each pixel has its own intensity and frequency value. There are So many algorithms which describe effective cryptographic system for data encryption that are considered operationally secure and are relatively difficult to break, but using cryptography does not necessarily assure security of a transmission. It creates some meaningless data after encryption which may found suspicious after malicious attack. That's why we have proposed image authentication technique with hiding codes by using stochastic diffusion encryption. The stochastic diffusion was first described as a population-based, pattern-matching algorithm. It belongs to a family of swarm intelligence and naturally inspired search and optimization algorithms which includes ant colony optimization, particle swarm optimization and genetic algorithms. Unlike the communication employed in ant colony optimization, which is based on modification of the physical properties of a simulated environment, stochastic diffusion uses a form of direct (one-to-one) communication between the agents similar to the tandem calling mechanism employed by one species of ants. Here we are using the stochastic diffusion for cryptography purpose. The same plain text should generate different cipher text even it is encrypted with same key. The diffusion ensures that the key is deriving the different cipher texts for same input contents. The same functioning should be done by the key while decrypting the text otherwise the attacker will easily break the encryption. He may make observation of input sent and output arrives and can make a partial guess of key used for encryption. At the initial stage diffusion technique provide the function of sensitivity to cryptographic system.

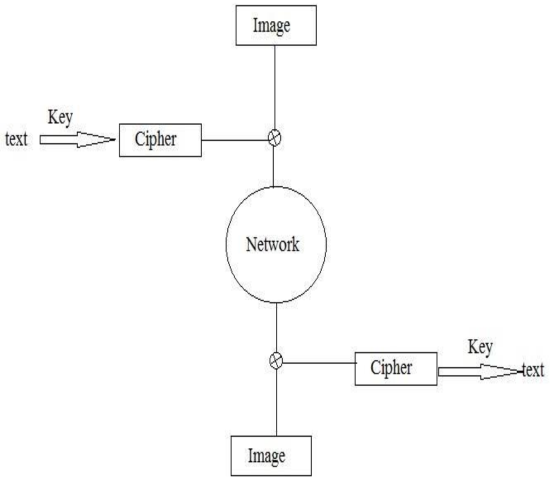


Figure 1 Traffic increases and need of Mobile Data Offloading

II. LITERATURE SURVEY

The previously published image authentication techniques dose not satisfies all the requirements. The pixel domain cannot be stored in the lossy compression format. The previous techniques produces the result but it is not much effective. Following are some previous techniques and their drawbacks.

[2.1] IMAGE AUTHENTICATION USING CRYPTOGRAPHY

The cryptography provides the better mechanism for information security. This technique uses the digital signature method to encrypt the image. Digital signature use to achieve private communication.

[2.1.1] DIGITAL SIGNATURE ALGORITHM

(i) GLOBAL PUBLIC-KEY COMPONENTS:

1. P = a prime number, where 2L-1 < p < 2L for 512 = < L= <1024 and L a multiple of 64
2. q = a prime divisor of p - 1, where 2159 < q < 2160
3. g = h(p-1)/q mod p, where h is any integer with 1 < h < p - 1 such that h(p-1)/q mod P>1(g has order q mod p).

(ii) THE USER'S PRIVATE KEY:

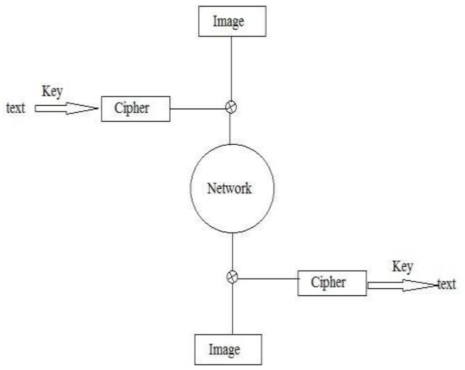
x = a randomly or pseudo randomly generated integer with 0 < x < q

(iii) USER'S PUBLIC KEY:

y = gx mod p

(iv) USER'S PER-MESSAGE SECRET NUMBER:

k = a randomly or pseudo randomly generated integer with 0 < k < q



[2.2] IMAGE AUTHENTICATION SYSTEM USING DISTRIBUTED SOURCE CODING

It provide a Slepian –Wolf encoded quantized image projection as authentication data. This version can be correctly decoded with the help of an authentic image as side information. Distributed source coding provides the desired robustness against legitimate variations while detecting illegitimate modification. The decoder incorporating expectation maximization algorithms can authenticate images which have undergone contrast, brightness, and affine warping adjustments

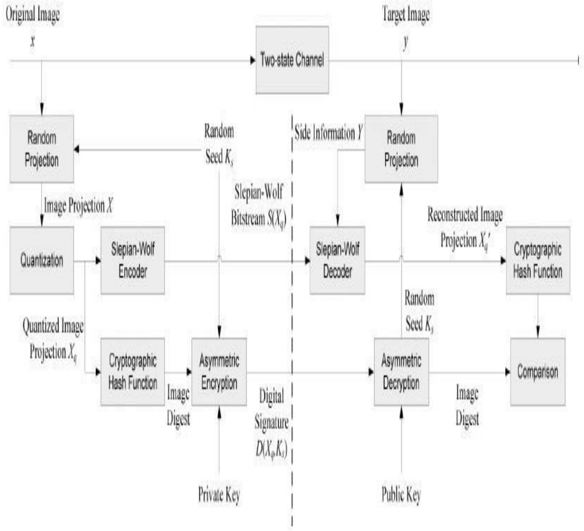


Figure: 3.Image Authentication using distributed source coding

[2.3] IMAGE AUTHENTICATION USING NEURAL NETWORK

Here, the media data, original authentication code and key are used to feed a neural network, which produces a secret parameter. Compared with media data, the secret parameter is of small size. Then, the secret parameter and the key are stored or transmitted in a secure way, while the media data are distributed freely. During distribution, media data may be tampered maliciously. In authentication, the received media data, secret parameter and key are used to feed the same neural network, which produces the computed authentication code. By comparing the original authentication code and the computed one, the authentication result is produced. That is, if there is only slight difference between them, then the multimedia data are not tampered, otherwise, they are tampered. To authenticate multimedia data successfully, two conditions are required. Firstly, the secret parameter and key are correct. Secondly, the received media data are same to or not very different from the original media data.

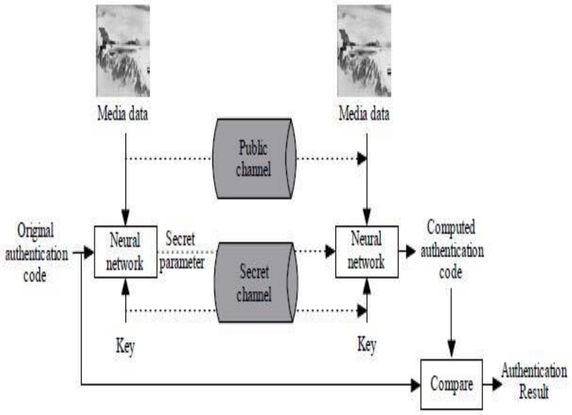


Figure: 4 Image Authentication using neural network.

[2.4] IMAGE AUTHENTICATION BASED ON DCT WITH RECOVERY CAPABILITY

In this paper an image authentication algorithm is proposed where the modified areas in an image are detected, and a digest image is recovered. Two different watermarks are used. One semi-fragile watermark is used for the authentication phase and is generated as a random sequence. The second watermark is use for making recovery efficient.

[2.4.1] WATERMARK GENERATION ALGORITHM

The first watermark *w*1 is generated as a random sequence using a key *k*1 similar to. In addition the second watermark *wdig* the digest image is generated as follows.

1. The original image is down-sampled by half to reduce the size; this is called *I*.

2. Subtract 127 from gray levels of *I* to force pixel values to be [-127,128]. This reduces theDCT coefficients values range.

3. *I* is divided in non-overlapping blocks of 8×8 pixels.

4. Compute the 2D-DCT of each block of 8×8.

5. The first sixteen DCT coefficients are retained from each block (1 DC coefficient and 15AC coefficients) in zig-zag order.

6. The DCT coefficient are rounded to the nearest integer and represented by 7 bits, including sign.

7. Before being encoded, DCT coefficients are quantized using the JPEG quantization matrix with quality factor equal to 50.

III. PROPOSED SYSTEM

The proposed method consists of information hiding strategy along with stochastic diffusion encryption. It consist of following methods

[3.1] HIDING OF ENCRYPTED INFORMATION

This can be classified into two types:

[3.1.1] HIDING IN SPATIAL DOMAIN

Here the host image is directly adjusted to lower computational cost. In this we are encrypting the image by using Advance Encryption Standard (AES). After that the generated watermark is compressed using arithmetic integer compression method. Then the compressed data retrieved is converted to a binary string and encoded in the image using the bit-plane which is specified by the user.

[3.1.2] HIDING IN TRANSFORM DOMAIN

In this transformation can be achieved by transforming the host image into a newly adjusted transform domain and then modifying the coefficients of image to embed information. This techniques require higher computational and operational cost and are more complex to implement, and they are assumed more robust to various attacks.

[3.2] HIDING OF ENCRYPTED INFORMATION USING STOCHASTIC DIFFUSION

The stochastic diffusion provides several advantages like it is the field of uniform diffusion and it can be computed by random number generator that can be used as private key for cryptography.

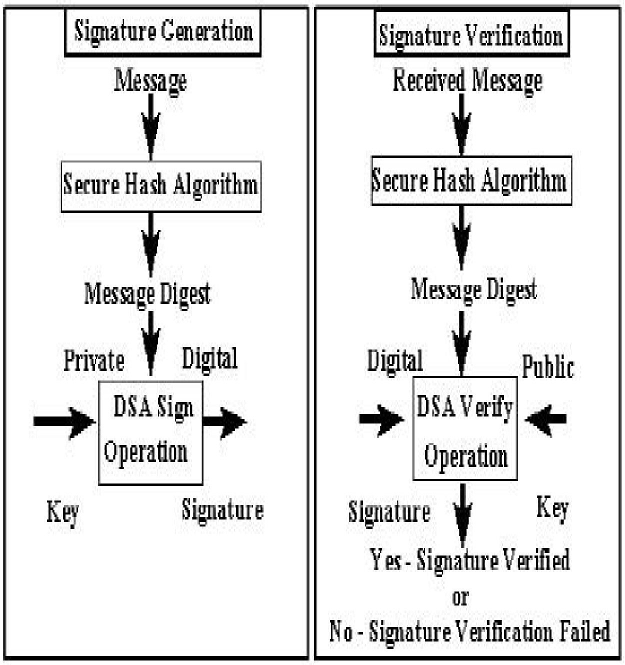
[3.3] HIDING CODES FOR BINARY IMAGE WATERMARKING

It is mainly used for extraction of LSB and to increase the security in hidden data and it improves the robustness of watermarking algorithm. Here we have considered three algorithms Gaussian distribution algorithm, Log-normal method, and Uniform distributions for generation of hidden codes.

[3.4] ENCRYPTED GREY SCALE IMAGE HIDING

In this the limitations of binary watermarking are overcome. The binarization cipher is not suitable for 8-bit images. In this we are hiding the 8-bit image into the 24-bit colour host image by using image scaling method. Firstly we converting cipher into binary form then its 1st ,2nd and last LSB are ignored.

3rd and 4th bit are embedded into two LSB. Other bits are embedded in the colour of the image.



IV. CONCLUSION

In this paper we have introduced an advanced encryption method using information hiding. The watermarking algorithm is only used for encryption purpose. But we have implemented the encoding technique of data hiding inside the image. The attacker will not able to decrypt the data until he extract it from image. It achieves security by hiding the encrypted data inside the host image. We have scaled the 8-bit image into 24-bit by using binarization and LSB property of the image. Which provides the high fidelity decrypt. The LSB compression method is use to avoid the full loss of the cipher bits. Because they are scattered along multiple bits. It will help to recover the original data hide inside the image.

V. REFERENCES

[1] R. Baeza-Yates and B. Ribeiro-Neto, Modern Information Retrieval. ACM Press, 1999.

[2] R. Baeza-Yates, C. Hurtado, and M. Mendoza, “Query Recommendation Using Query Logs in search Engines,” Proc. Int’l Conf. Current Trends in Database Technology (EDBT ’04), pp. 588-596, 2004.

[3] D. Beeferman and A. Berger, “Agglomerative Clustering of a Search Engine Query Log,” Proc. Sixth ACM SIGKDD Int’l Conf. Knowledge Discovery and Data Mining (SIGKDD ’00), pp. 407-416, 2000.

[4] S. Beitzel, E. Jensen, A. Chowdhury, and O. Frieder, “Varying Approaches to Topical Web Query lassification,” Proc. 30th Ann. Int’l ACM SIGIR Conf. Research and Development (SIGIR ’07), pp. 783-784, 2007.

[5] H. Cao, D. Jiang, J. Pei, Q. He, Z. Liao, E. Chen, and H. Li, “Context-Aware Query Suggestion by Mining Click-Through,” Proc. 14th ACM SIGKDD Int’l Conf. Knowledge Discovery and Data Mining (SIGKDD ’08), pp. 875-883, 2008.

[6] H. Chen and S. Dumais, “Bringing Order to the Web: Automatically Categorizing Search Results,” Proc. SIGCHI Conf. Human Factors in Computing Systems (SIGCHI ’00), pp. 145-152, 2000.

[7] C.-K Huang, L.-F Chien, and Y.-J Oyang, “Relevant Term Suggestion in Interactive Web Search Based on Contextual Information in Query Session Logs,” J. Am. Soc. for Information Science and Technology, vol. 54, no. 7, pp. 638-649, 2003.

[8] T. Joachims, “Evaluating Retrieval Performance Using Clickthrough Data,” Text Mining, J. Franke, G. Nakhaeizadeh, and I. Renz, eds., pp. 79-96, Physica/Springer Verlag, 2003.

[9] T. Jachims, “Optimizing Search Engines Using Clickthrough Data,” Proc. Eighth ACM SIGKDD Int’l Conf. Knowledge Discovery and Data Mining (SIGKDD ’02), pp. 133-142, 2002.

[10] T. Joachims, L. Granka, B. Pang, H. Hembrooke, and G. Gay, “Accurately Interpreting Clickthrough Data as Implicit Feedback,” Proc. 28th Ann. Int’l ACM SIGIR Conf. Research and Development in Information Retrieval (SIGIR ’05), pp. 154-161, 2005.

[11] R. Jones and K.L. Klinkner, “Beyond the Session Timeout: Automatic Hierarchical Segmentation of Search Topics in Query Logs,” Proc. 17th ACM Conf. Information and Knowledge Management.