International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 8 Issue 11, November-2019

Development of Harmonic Model for Secured Multimedia Application in Grid Computing

Harmonic Model for Secured Multimedia in Grid Computing

Dr. Purohit Shrinivasacharya
Information Science and Technology
SIT, Belgaum

Prof. Krishna R. Kulkarni
CSE
ICOER, Pune

Mr. Piyush Thada
ICOER, Pune

Mrs. Aishwarya Mule
ICOER, Pune

Mrs. Diksha Wagh
ICOER, Pune

Mrs. Priya Rathod
ICOER, Pune

***Abstract*—In recent year cloud computing is trend in networking industry. The storing data in the cloud can alleviate the storage overhead and reduce the expense of the both hardware and software for the individuals. Today's world, visual cryptography is the technique used to transmit the secret information by encrypting into images called secret image cryptography, this is the recent trend in the field of information secured technology. The research has been proposed to design and develop energy efficient and high-speed architecture for secure multimedia applications using visual cryptography. DES algorithm is used for encryption which is most secured algorithm, Grid computing is used to provide high performance computing power enormous data storage, which will be arrange in matrix form. In this network to get the fast access, grid computing plays an important role. Our proposed new model provides high security and access to the harmonic mean average, which provides the key for searching and is helpful to find the files on cloud)**

Keywords—FPGA; Cloud computing; Fuzzylogic; grid computing; security; harmonic function

1. INTRODUCTION

Transmission of multimedia data through network has been increased rapidly in 21st century to provide instant access of digital data. The transmission of multimedia data over network demand considerable security and it is very important in sharing personal information through public networks. In literature there were many security methodologies developed by researcher. However, security can be provided to the multimedia data in many ways such as transmitting along with password, image hiding, watermarking, authentication and identification. But these techniques cannot protect secret information when transmitted through single information carrier. If the carrier is lost once, the information may be either damaged or destroyed. In recent days, visual cryptography is the technique used to transmit the secret information by encrypting into images called secrete image. The sharing of secret images over public network is an important and recent trending the field of communication technology, information security and production.

With the increasing requirements for more flexibility and higher performance in embedded systems design, a new computing paradigm reconfigurable architecture such as Field Programmable Gate Array (FPGA) promises greater flexibility without compromise in performance and flexibility. The FPGA contains both memory and logic elements along with an intellectual property (IP) processor core to rapidly implement a computer and custom hardware for high speed embedded systems. So complex applications, like computation intensive kernels, MIMO, OFDM and image processing are accelerated by reconfigurable architecture and achieved higher performance by reducing the instruction fetch, decode and execute bottleneck. The FPGA brings the phenomenon of configuring custom digital circuits dynamically and modified via software. This ability of creating and modifying digital logic circuits without physically altering the hardware provides more flexible and low-cost solution for real time applications. So High Speed Computing Systems (HSCS) should have one or more resources of such kind as PE to enhance the speed of real time application. This phenomenon of dynamic reconfiguration of an application is enabled by the availability of high-density programmable logic chips FPGA. The FPGA architecture is available in two forms.

Fine-grained FPGA Architecture: An FPGA consists of a matrix of programmable logic cells with a grid of interconnecting lines running between them. In addition, there are I/O pins on the perimeter that provide an interface between the FPGA, the interconnecting lines and the chip's external pins. However, FPGAs tend to be somewhat fine-grained in order to achieve high degree of flexibility. This flexibility has its place for situations where the computational requirements are either not known in advance or vary considerably among the needed applications. However, in many cases this extreme level of flexibility is unnecessary and would result in significant overheads of area, delay and power consumption. Today, further improvements are being made by embedding coarse-grained elements such as memories, multipliers, and processors within the fine-grained programmable fabric of the FPGA. Coarse-grained FPGA Architecture: Contrasted with Fine-grained FPGAs, the data-path width of coarse-grained elements of reconfigurable architectures is more than one bit. Over the last 15 years, many projects have been investigated and successfully built systems based on Coarse-grained reconfiguration performed within a processor or amongst processors. The Coarse-gained reconfiguration procedure is much faster than that found in Fine-grained FPGAs. The Coarse- grained elements can implement a specific function more efficiently than Fine-grained programmable logic. However, since Coarse-gained FPGA architecture is not as flexible, they only benefit applications which utilize them. In this thesis, Coarse-grained elements required for targeted computing architecture is configured on Fine-grained FPGA architecture to support faster execution of real-life applications.

This research has been proposed to design and develop energy efficient and high-speed architecture for secure multimedia applications using visual cryptography. In this research, a hardware model will be developed for the behavior of visual cryptography to encrypt the multimedia data such as images and audio information.

2. LITERATURE REVIEW

Visual cryptography encodes a secret binary image into n shares of random binary patterns. Since the shares which are XORed onto transparencies many do not have visual meaning and hinder the objectives of visual cryptography. A novel technique called halftone visual cryptography has been proposed into achieve visual cryptography via half toning. The proposed method utilizes the void and cluster algorithm to encode a secret binary image into n halftone shares (images) carrying significant visual information. Transparency of pixels of the shares can reveal the secret image. The pixels of shares of an image can be generated randomly, on the other hand the cover image also could play significant role in generation of the first share. The encrypted shares generated by cover image looks like visually less similar as compared to those shares generated without using cover image. The method proposed in encourages the use of properly selected cover image for visual cryptography with pixel transparency. Preserving the privacy of digital biometric information, i.e. face images, stored in a central database has become supreme importance. In, a visual cryptography framework has been proposed for providing privacy to biometric information such as fingerprint, iris codes, and face images. The private face image is partition into two face images sheets and the image sheets are stored in two independent database servers. The individual sheet of private image does not support the reveal of its identity. The private image can be reconstructed only when both sheets are available simultaneously. A series of experiments on the face image databases demonstrated the following:

1. Possibility of hiding a private face image in two image sheets.
2. Successful matching of private face images sheet and reconstruction.
3. Inability of individual sheets of private image to reveal the identity of the private face image.
4. The difficulty of cross database matching for determining identities.

A similar process can be used for fingerprint images and iris codes before storing them in a central database.

The research in demonstrated the problem of encrypting a privacy binary image into n shares of meaningful halftone images using the scheme visual cryptography. The noise introduced during encryption of secret pixels can be nullified into neighboring pixels while enhancing halftone shares. The Visual cryptography has not performed significant role in real time applications because of its difficulty in practice. The shares of visual cryptography are printed on transparencies which needed to be superimposed. However, the precise superimposition is not very easy to do because of the fine resolution as well as printing noise. Furthermore, many visual cryptography applications need to print shares on paper in which scanning of the share is necessary. The print and scan process can introduce noise as well which can make the alignment difficult. In authors have developed a frequency domain alignment scheme to find the alignment position of these shares. Authors in discuss how to use the visual cryptography in watermarking technique. The authors proposed a joint visual-cryptography and watermarking (JVW) algorithm that has the merits of both visual cryptography and watermarking. Both halftone watermarking and visual cryptography involve a hidden secret image and the hidden image can only be revealed when enough shared images are obtained. Authors in have proposed a new method of visual cryptography scheme to encode the encoded n shares into number of sub shares recursively in order to increase the level of security of the encrypted message. In, a robust copyright protection scheme was proposed by using the watermarking technique to generate a secret image and a public image by using the visual cryptography technique. The secret image further can be registered as image to certified authority **(CA)**to provide protection. Wherein, the watermarking image has been acquired by performing exclusive-OR **(XOR)** operation on the secret image and the public image. The beauty of VCS scheme enables recovery of the secret image without any cryptographic knowledge and computation devices. An extended visual cryptography scheme (EVCS) [11] is presented by embedding random shares into meaningful covering shares. Visual cryptography is cryptography where n images are encoded in such a way that human only can visualize the decrypted hidden message without any cryptographic computations. In authors have presented an improved algorithm scheme for hiding a color image into multiple color cover images in order to achieve lossless recovery without any additional computational complexity. Recently, a rapid growth has happened in E-Commerce market around the globe. The popularity of online shopping has faced many security issues like Debit or Credit card fraud and personal information security and the issues has become major concerns of customers, merchants and banks.

In a novel copyright protection scheme is proposed that combines the discrete wavelet transform (DWT) and the singular value decomposition (SVD). Instead of modifying the original host image to conceal a secret image, the proposed scheme first extracts the image features from the host image by applying the DWT and the SVD. The extracted features are then classified into two clusters by employing the k-means clustering technique, and a master share is generated using the clustering result. The identified master share is then used together with a secret image to construct an ownership share using visual cryptography (VC) technique. When rightful ownership needs to be determined, the secret image for ownership identification can be revealed by stacking the master share and the ownership share. Experimental results demonstrated that the proposed scheme can effectively resist several common attacks.

3. OBJECTIVE OF THE RESEARCH WORK

Since the FPGA devices provides energy efficient and high-speed solutions for real time embedded applications, this research is proposed with the objective of developing Visual Cryptography framework on FPGA for secure multimedia applications.

In this research, hardware architecture is described for the Visual Cryptography Scheme and implemented on FPGA in order to bring energy efficiency and also enhance the execution speed of multimedia applications.

Finally, the proposed Visual Cryptography architecture will be applied for secure multimedia data storage and transmission.

4. PROBLEM FORMULATION

A. System Model

In this paper, we consider a data system consisting of data owner, data user and server. Given a collection of n encrypted data files C = (F$_1$, F$_2$, . . ., F$_N$) stored in the server, a predefined set of distinct keywords W= {w$_1$, w$_2$, ..., wp$^}$, the server provides the search service for the authorized users over the encrypted data C. We assume the authorization between the data owner and users is appropriately done. An authorized user types in a request to selectively retrieve data files of his/her interest. The server is responsible for mapping the searching request to a set of data files, where each file is indexed by a file ID and linked to a set of keywords. The fuzzy keyword search scheme returns the search results according to the following rules: 1) if the user's searching input exactly matches the pre-set keyword, the server is expected to return the files containing the keyword; 2) if there exist typos and/or format inconsistencies in the searching input, the server will return the closest possible results based on pre-specified similarity semantics (to be formally defined in section III-D).

B. Threat Model

We consider a semi-trusted server. Even though data files are encrypted, the server may try to derive other sensitive information from users' search requests while performing keyword-based search over C. Thus, the search should be conducted in a secure manner that allows data files to be securely retrieved while revealing as little information as possible to the server. In this paper, when designing fuzzy keyword search scheme, we will follow the security definition deployed in the traditional searchable encryption. More specifically, it is required that nothing should be leaked from the remotely stored files and index beyond the outcome and the pattern of search queries.

C. Design Goals

In this project, we address the problem of supporting efficient yet privacy-preserving fuzzy keyword search services over encrypted data. Specifically, we have the following goals: i) to explore new mechanism for constructing storage efficient fuzzy keyword sets; ii) to design efficient and effective fuzzy search scheme based on the constructed fuzzy keyword sets; iii) to validate the security of the proposed scheme.

D. Preliminaries

There are several methods to quantitatively measure the string similarity. In this paper, we resort to the well-studied edit distance for our purpose. The edit providing an overview of how fuzzy search scheme works over encrypted data. Assume Π=(Setup(1λ$_)$, Enc(sk,), Dec(sk,)) is a symmetric encryption scheme, where sk is a secret key, Setup(1λ$_)$ is the setup algorithm with security parameter λ, Enc (sk, λ1) and Dec (sk, λ2) are the encryption and decryption algorithms, respectively. Let Tw$_i$ denote a trapdoor of keyword wi. Trapdoors of the keywords can be realized by applying a one-way function f, which is similar as Given a keyword wi and a secret key sk, we can compute the trapdoor of wi as Tw$_i$= f (sk, wi$^)$. We begin by constructing the fuzzy keyword set Swi, d for each keyword wi∈W (1≤ i≤ p) with edit distance d. The intuitive way to construct the fuzzy keyword set of wi is to enumerate all possible words w$_i$′ that satisfy the similarity criteria ed (wi, ^{w}i′$_)$ ≤ d, that is, all the words with edit distance d from wi are listed. For example, the following is the listing variants after a substitution operation on the first character of keyword: -

CASTLE: {AASTLE, BASTLE, DASTLE, ZASTLE}.

Based on the resulted fuzzy keyword sets, the fuzzy search over encrypted data is conducted as follows:

1) To build an index for wi, the data owner computes trapdoors Tw′$^=$f (sk, w′$_i$) for each w′$_i$∈Swi, d with a secret distance ed (w$_1$, w$_2$) between two words w$_1$and w$_2$is the number of operations required to transform one of them into the other. The three primitive operations are 1) Substitution: changing one character to another in a word; 2) Deletion: deleting one character from a word; 3) Insertion: inserting a single character into a word. Given a keyword w, we let Sw, d denote the set of words w′ satisfying ed (w, w′$_)$ ≤ d for a certain integer d. Using edit distance, the definition of fuzzy keyword search can be formulated as follows: Given a collection of encrypted data files C = (F$_1$, F$_2$, . . . , FN$^)$ stored in the server, a set of distinct keywords W= {w$_1$, w$_2$, ..., wp$^}$with predefined edit distance d, and a searching input (w, k) with edit distance k(k≤d), the execution of fuzzy keyword search returns a set of file IDs whose corresponding data files possibly contain the word w, denoted as F IDw: if w = wi∈W , then return F IDw$_i$; otherwise, if w 6∈ W, then

return {F IDw_i}, where ed(w, wi$^{)}$≤ k. Note that the above definition is based on the assumption that k ≤ d. In fact, d can be different for distinct i key sk shared between data owner and authorized users. The data owner also encrypts FID$_w$i^{as}Enc(sk, FID$_w$i^{k}wi$^)$.

The index table {({Tw$_i$′$^{\}}$w′$_i$∈Swi,d'Enc(sk, FID$_w$i^{k}wi$^{))}$}wi∈W and encrypted data files are outsourced to the server for storage; 2) To search with w, the authorized user computes the trapdoor Tw of w and sends it to the server; 3) Upon receiving the search request Tw, the server compares it with the index table and returns all the possible encrypted file identifiers {Enc(sk, FID$_w$i^{k}wi$^)$} according to the fuzzy keyword definition in section III-D. The user decrypts the returned results and retrieves relevant files of interest. This straightforward approach apparently provides fuzzy keyword search over the encrypted files while achieving search privacy using the technique of secure trapdoors. However, this approach has serious efficiency disadvantages. The enumeration method in constructing fuzzy keyword sets would introduce large storage complexities, which greatly affect the usability. Recall that in the definition of edit distance, substitution, deletion and insertion are three kinds of operations in computation of edit distance. The numbers of all similar words of wi satisfying ed(wi, $^{w'}{}_i$)≤ d for d = 1, 2 and keywords and the system will return {F IDwi$^{\}}$satisfying approximately2k × 26,2k^2× 26^2, and^{4}3^k 3× 26^3,ed(w, wi$^)$≤ min{k, d} if exact match fails.

5. MOTIVATION / PROBLEM STATEMENT DEFINITION

The Visual Cryptography is a method of encrypting secret image into n number of random shares and distribute to the n number of entities. The encrypted secret image can be decrypted by stacking the distributed random shares from the n number of entities. Visual Cryptography can also be applied to encrypt the secret information into an image. However, the Visual Cryptography Scheme (VCS) suffers from security because of its software implementation. Since the software model of VCS could run-on general-purpose processor requires more power energy and also leave space for security issues. So, this research is motivated to develop high speed and energy efficient hardware system for secure multimedia applications.

6. PROPOSED RESEARCH METHODOLOGY

The data flow of the proposed Visual Cryptography architecture for secure multimedia transmission is described in figure 1. The architecture uses a well-known compression scheme to compress the size of the secret shares. Since the embedding process increases the execution time of the entire system and also degrades the quality of the regenerated image, FPGA devices are selected as computing platform. The proposed system provides an integrated environment to process images and it supports only single image format either .gif or .png. The proposed system consists of three basic operations these are compressed share generation, encoding and decoding. Encoding is done by secret share generation and compression of these secret shares. Decoding is done by the stacking of the secret shares at the receiver's end.

Figure 1: Visual Cryptography Architecture for multimedia applications

The data flow of the cryptographic process is demonstrated and the sequence of steps

1. Select the image as input
2. Create encrypted shares using an appropriate encoding algorithm for intended secret image.
3. Prepare the dictionary for encrypted shares.
4. In dictionary replaces strings of characters with Single codes.
5. In the compression of encrypted share, select the secret pixels.
6. Then generation halftone shares using error diffusion Method.
7. Filter process is applied to the output encrypted shares.
8. Filters are used to improve the quality of the reconstructed image to minimize the noises for sharpening the input secret image.

The proposed architecture is then used for processing multimedia data like images, video and audio information.

7. POSSIBLE OUTCOME / RESULT

An energy efficient architecture for visual cryptography framework to store and transmit secure multimedia data over wired channel.

Estimation of hardware resources required for the proposed architecture and comparison statement with contemporary architectures in literature.

Estimation of the performance attributes like speed, memory and data handling capacity of the proposed architecture.

8. CONCLUSIONS

Literature review on the visual cryptographic has been done for multimedia data storage and transmission. The literature review also completed on computing systems and FPGA device is chosen as computing platform for implementing the proposed architecture. The proposed architecture for secure multimedia data transmission has simple mathematical calculations and that provides solutions for multimedia applications at optimum energy efficiency and enhanced speed.

9. REFERENCES

[1] Zhi Zhou, G. R. Arce and G. Di Crescenzo, "Halftone visual cryptography," in IEEE Transactions on Image Processing, vol. 15, no. 8, pp. 2441-2453, Aug. 2006.

[2] D. Shrestha and S. P. Panday, "Visual cryptography using image pixel transparency with cover image," 2015 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), Kathmandu, 2015, pp. 1-4.

[3] A. Ross and A. Othman, "Visual Cryptography for Biometric Privacy," inIEEE Transactions on Information Forensics and Security, vol. 6, no. 1, pp. 70-81, March 2011.

[4] Z. Wang and G. R. Arce, "Halftone Visual Cryptography Through Error Diffusion," 2006 International Conference on Image Processing, Atlanta, GA, 2006, pp. 109-112.

[5] Wei-Qi Yan, Duo Jin and M. S. Kankanhalli, "Visual cryptography for print and scan applications," 2004 IEEE International Symposium on Circuits and Systems (IEEE Cat. No.04CH37512), 2004, pp. V-572-V-575

[6] Ming Sun Fu and O. C. Au, "Joint visual cryptography and watermarking," 2004 IEEE International Conference on Multimedia and Expo (ICME) (IEEE Cat. No.04TH8763), Taipei, 2004, pp. 975-978 Vol.2.

[7] T. Monoth and A. P. Babu, "Recursive Visual Cryptography Using Random Basis Column Pixel Expansion," 10th International Conference on Information Technology (ICIT 2007), Orissa, 2007, pp. 41-43.

[8] Der-Chyuan Lou, Hao-Kuan Tso, Jiang-Lung Liu, A copyright protection scheme for digital images using visual cryptography technique
Computer Standards & Interfaces, Volume 29, Issue 1, Pages 125-131.

[9] Young-Chang Hou and Pei-Min Chen, "An asymmetric watermarking scheme based on visual cryptography," WCC 2000 - ICSP 2000. 2000 5th International Conference on Signal Processing Proceedings. 16th World Computer Congress 2000, Beijing, 2000, pp. 992-995 vol.2.

[10] F. Liu and C. Wu, "Embedded Extended Visual Cryptography Schemes," in IEEE Transactions on Information Forensics and Security, vol. 6, no. 2, pp. 307-322, June 2011.

[11] R. Youmaran, A. Adler and A. Miri, "An Improved Visual Cryptography Scheme for Secret Hiding," 23rd Biennial Symposium on Communications, 2006, Kigston, Ont., 2006, pp. 340-343.

[12] J. Weir and W. Yan, "Sharing multiple secrets using visual cryptography," 2009 IEEE International Symposium on Circuits and Systems, Taipei, 2009, pp. 509-512.

[13] S. Roy and P. Venkateswaran, "Online payment system using steganography and visual cryptography," Electrical, Electronics and Computer Science (SCEECS), 2014 IEEE Students' Conference on, Bhopal, 2014, pp. 1-5.

[14] Ming-Shi Wang, Wei-Che Chen, A hybrid DWT-SVD copyright protection scheme based on k-means clustering and visual cryptography
Computer Standards & Interfaces, Volume 31, Issue 4, Pages 757-762.

[15] Makimoto, T., "The hot decade of field programmable technologies," Proceedings of IEEE International Conference onField-Programmable Technology, 16-18 Dec. 2002, pp.3 – 6.

[16] Yuanqing Guo, Mapping Applications to a Coarse-Grained Reconfigurable Architecture, PhD thesis.

[17] Ganghee Lee, Kiyoung Choi and Nikil D. Dutt, “Mapping Multi-Domain Applications onto Coarse-Grained Reconfigurable Architecture, IEEE Transactions on Computer Aided Design of Integrated Circuits and Systems, Vol. 30, No. 5, May 2011.

[18] Chao-Yang Kao and Youn-Long Lin, “A Memory-Efficient and Highly Parallel architecture for Variable Block Size Integer Motion Estimation in H.264/AVC”, IEEE Transactions on Very Large-Scale Integration (VLSI) Systems, Vol. 18, No. 6, June 2010

[19] D. Wang, S. Li and Y. Dou, “Loop Kernel Pipelining Mapping onto Coarse-Grained Reconfigurable Architecture for Data-Intensive Applications,” Journal of Software, Volume 4, no-1, p81-89, 2009.

I. Reiner Hartensstein, “Microprocessor is no more General Purpose: Why future reconfigurable platforms will win,” invited paper of the International