Design and Analysis of an Image Encryption Using Digital Signature

Onyedeke, Obinna Cyril[1], Ihedioha Uchechi. M[2], Emmanuel C Osinem[3], Atanda Aminat Oluchi[4], Ogbene Nnaemeka Emeka[5], Nnamdi Johnsom Ezeora[6], Agubata Immaculate Chidimma[7], Egbugo Collins T[8], Anichebe E. Gregory[9]

[1,7]*Department of Computer Science University of Kairouan, Tunisia*
[2, 4,5,6,8,9] *Department of Computer Science University of Nigeria, Nsukka, Nigeria*
[3]*Department of Agricultural education/Vocational Technical education, University of Nigeria, Nsukka, Nigeria*

Abstract: **In the world today, web is presently going ahead from text information to media information; one of the significant security concerns is the assurance of this multimedia information. Image, which covers the most elevated level of the multimedia information, its security is significant. This can be accomplished by Image encryption. This paper contribution is geared towards securing image transmission using digital signature of the original image by encoding version of original image, the encoding of the images is done using an error control code. The goal of this paper is to develop a system that uses a symmetries method (Encryption and Decryption) for an image and also platform that convert image into string (Alphanumeric Strings). The technique used is digital Signature which enables the recipient of a message to authenticate the sender of a message and verify that the message is intact and it creates new symmetric block encryption schemes. An error control code is determined in real-time on the size of the original image.**

Keywords: **Image Encryption, Digital signature, Decryption, Multimedia security.**

I. INTRODUCTION

With the ever-expanding development of multimedia applications, security is a significant issue in correspondence and capacity of images, and encryption is one the approaches to guarantee security. Image encryption strategies attempt to change over unique image to another image that is difficult to comprehend; to keep the image classified between clients, in other word, it is basic that no one could become more acquainted with the substance without a key for decoding. Besides, extraordinary and solid security in Storage and transmission of computerized images is required in numerous applications, for example, satellite TV, online individual photo collection, clinical imaging frameworks, military image interchanges and classified video gatherings, and so on. So as to satisfy such an assignment, many picture encryption strategies have been proposed. The image encryption calculations can be characterized into three significant gatherings: position stage based calculation, esteem change based calculation and visual change based calculation [1]. With the development of Networks and the rising measure of data that we live with. These days, new systems of data handling are developing so as to advance. The transmission and the capacity of data. The limit of transmission and capacity is developing, however so are the measures of data with which we are managing. It is here, where pressure gets important. While thinking about information pressure, we discover the absolute most significant applications to the fields of multimedia. This is on the grounds that those records contain high measures of data; in that capacity, engineers are scanning for proficient approaches to diminish it. In this task we center on image pressure (Encryption and Decryption). Images that we will pack with our created calculations. In sections three and four we present the lossless and lossy pressure methods from which our calculations have been motivated.

One of the principle objectives of this paper was is to get familiar with Fractal pressure and fractals as a rule. From that point onward, I felt that it could be intriguing to build up a JPEG calculation, as these days it is one of the most broadly utilized pressure strategies. The objective was to think about those two lossy pressure plans and different lossless pressure methods so as to get a worldwide vision of the subject. Individuals intrigued by the subject can get a first thought of the pressure accomplished when utilizing every last one of the pressure plans and arrive at resolutions dependent on the relative examination [2]. Different parts, for example, the foundation or the appearance in the mirror are hazy. Lenna is an image with various degrees of difference and brilliance; the brightening originates from various focuses, and we can see this in the cap and her face. The image contains a decent blend of subtleties, and for each one of those reasons, this picture is to a great extent utilized in the realm of picture pressure (www.wikipedia.org/wiki/jpeg). Additionally it is gainful to have a typical picture to pack in established researchers so as to test the calculations. On account of Lenna it is anything but difficult to assess the outcomes and the effectiveness of an allowed calculation since we get the opportunity to contrast the aftereffects of this calculation and the consequences of other significant calculations that has been utilized to pack the very same picture.

II. SECURITY ISSUES ON IMAGE

Multimedia security in general is provided by a method or a set of methods used to protect the multimedia content. These techniques are vigorously founded on cryptography and they empower either correspondence security, or protection from theft (Digital Rights Management and watermarking), or both. Correspondence security of computerized pictures and literary advanced media can be cultivated by methods for standard symmetric key cryptography. Such media can be treated as double succession and the entire information can be scrambled utilizing a cryptosystem, for example, Advanced Encryption Standard (AES) or Data Encryption Standard (DES) [3]. By and large, when the interactive media information is static (not an ongoing gushing) it can rewarded as an ordinary double information and the customary Encryption methods can be utilized. Settling on what level of security is required is harder than it looks. To recognize an ideal security level, the expense of the sight and sound Information to be ensured and the expense of the assurance itself are to be thought about cautiously.

2.1 A Technique for Image Encryption Using Digital Signature

In this scheme, according to [4] have proposed a new technique to encrypt an image for secure image transmission using digital signature of the original image is added to the encoded version of original image, the encoding of the images is done using an error control code. An error control code is determined in real-time on the size of the original image. The digital Signature enables the recipient of a message to authenticate the sender of a message and verify that the message is intact. Create new symmetric block encryption schemes. A chaotic map is generalized by introducing parameters and then discredited to a square lattice of points which represent pixels or some other data items. Although the discredited map is a permutation and thus cannot be chaotic, it shares certain properties with its continuous counterpart as long as the number of iterations remains small.

2.1.2 Theoretical Framework

Multimedia security in general is provided by a method or a set of methods used to protect the multimedia content. These methods are heavily based on cryptography and they enable either communication security, or security against piracy (Digital Rights Management and watermarking), or both. Communication security of digital images and textual digital media can be accomplished by means of standard symmetric key cryptography. In general, when the multimedia data is static (not a real-time streaming) it can treated as a regular binary data and the conventional encryption techniques can be used. Deciding upon what level of security is needed is harder than it looks. To identify an optimal security level, the cost of the multimedia information to be protected and the cost of the protection itself are to be compared carefully.

2.2 Review of Related Literatures

This section, examines a portion of the past methodologies used by researchers for image encryption and decryption. Below, we give a concise survey of research studies that have been conducted on image encryption of existing systems.

According to [5], Analyzed Energy Consumption of RC4 and AES Algorithms in Wireless LANs. RC4 and AES encryption calculations execution assessment is made by their exploration. The measurements for such assessment are as per the following: CPU outstanding task at hand, encryption throughput, key size variety and vitality cost. Exploratory outcomes reason that for encoding huge bundles the RC4 is vitality effective and quick. Be that as it may, for a littler parcel size encryption AES was more productive than RC4. Subsequently apparently by utilizing a mix of RC4 and AES we can spare vitality to give encryption to any bundle size.

In [6], proposed an image encryption by a tumultuous neural framework and the feline guide. Disarray procedure was utilized in making the neural systems and J. Procedure for Image Encryption.

According to [7], proposed another exceptionally enhanced picture calculation utilizing stage and replacement strategies. It was done so as to improve the pseudorandom qualities of tumultuous groupings, a streamlined treatment and a cross-testing removal is utilized K. Method for Image Encryption utilizing confusion procedure.

In [8], proposed a calculation utilizing two riotous frameworks. One riotous framework creates a confused grouping, which was changed into a double stream utilizing a limit work. The other disordered framework was utilized to develop a change grid. . Initially, utilizing the twofold stream as a key stream, haphazardly the pixel estimations of the pictures was altered. At that point, the adjusted image was scrambled again by stage lattice.

As indicated by [9], Proposed a made sure about cryptographic change (encryption or unscrambling) of one fixed length gathering of bits called a square is the main capacity performs by square figure. To safely change measures of information bigger than a square it is expected to over and over apply figure's single-square activity. The technique of applying this activity is portrayed by method of activity calculation.

In [10], introduced another method to encode a picture for secure picture transmission. The advanced mark of the first picture is added to the encoded rendition of the first picture. Picture encoding is finished by utilizing a fitting mistake control code, for example, a Bose-Chaudhuri Hochquenghem (BCH) code. At the beneficiary end, after the unscrambling of the picture, the advanced mark can be utilized to confirm the credibility of the picture.

According to [11], proposed an algorithm which performs both lossless pressure and encryption of double and dim scale pictures. The pressure and encryption plans depend on SCAN designs created by the SCAN approach. The SCAN is a conventional language-based two-dimensional spatial-getting to procedure which can effectively determine and produce a wide scope of filtering ways or space filling bends.

In [12], proposed an effective mirror-like picture encryption calculation. In light of a double arrangement created from a turbulent framework, a picture is mixed by the calculation. This calculation comprises of 7 stages. Step-1 decides a 1-D disordered framework and its underlying point x (0) and sets k = 0. Step-2 produces the disorderly succession from the turbulent framework. Step-3 produces parallel arrangement from disordered framework. Steps-4,5,6, and 7 modify picture pixels utilizing trade work as indicated by the double succession.

According to [13], presents a presentation assessment of chose symmetric encryption calculations on power utilization for remote gadgets in their paper named "Assessing the Effects of Cryptography Algorithms on power utilization for remote gadgets." following focuses are closed by him from his trial result. 1) If parcel size is changing with or without transmission of information utilizing different WLANs conventions and various designs. It was finished up structure the outcome that Blowfish and AES has preferable execution over other basic encryption calculations utilized, trailed by RC6. Worm gaps are available in the security system of DES and 3DES; Blowfish and AES don't have such worm gaps any up until now.

In [14], proposed another image encryption plot dependent on a tumultuous framework. In their strategy, a capricious disordered succession is produced. It is utilized to make a double succession once more. As per the double grouping, a picture's pixels are modified. This calculation has four stages. Step-1 0064zAetermines a confused framework and its underlying point x (0), line size M and segment size Not the image f, iteration number no, and constants Į,ù, and µ used to decide the revolution number. Step-2 produces the disordered grouping from the disorganized framework. Step-3 produces the twofold grouping. Step-4 incorporates unique capacities to adjust picture pixels.

III. ANALYSIS OF THE PROPOSED WORK

System analysis is a procedure of social affair and deciphering realities, diagnosing issues and the data to suggest enhancements for the framework. It is a critical thinking action that requires serious correspondence between the framework clients and framework engineers. When partners have been perceived, the social event and investigation of the necessities can start. Necessity gathering must be identified with business needs or openings. Prerequisite examination includes catching necessities and investigating prerequisites. Catching necessities is speaking with partners to concur on what the prerequisites are. Examining necessities is utilizing standard devices to create a gauge of the prerequisites. Once the stakeholders concur on the requirements, the baseline is created and becomes the formal requirement source. Within this analysis phase, the analyst is discovering and fact finding. Along with meeting with stakeholders, the analyst must meet with end users to understand what the user's needs are and to learn about problems that affect the current system in order to assist with designing a new and more efficient system. There are several activities that must occur within the analysis phase:

1. Gather Information
2. Define the new system's requirements
3. Build prototypes for the new system
4. Prioritize requirements
5. Evaluate alternatives
6. Meet with management to discuss new options

3.1 Design of the Proposed System

A web base application designed and developed with python flask framework, that convert digital image into alphanumeric string and send through network (Localhost/Hosted). Images are not recognized by the user. This paper aimed at providing high security for the digital images data and keeping them from spying. It also aims at getting encryption algorithm accuracy and safety features and maintaining the images data from loss when decryption process. Image encryption is one of the most important applications in transferring images through the internet and cellular phones. The design and implement of this system has the following objectives:

1. To develop a system that uses a symmetries method (Encryption and Decryption) for an image
2. To develop a platform that convert image into string (Alphanumeric Strings)
3. To develop web based application to perform above listed objective

3.2 Process Design

The process of the system functionality can be presented in several ways. However, for the purpose of this paper, the researcher made use of system structure chart (flow chart) and the Data flow diagram to depict the process design.

Data flow diagram: The DFD is a graphical representation of a system that shows the inputs to the system, the processing upon the inputs, the outputs of the system as well as the internal data stores. Rumbaugh et al. defined DFD as, “A data flow diagram is a graph which shows the flow of data values from their sources in objects through processes that transform them to their destinations on other objects.”

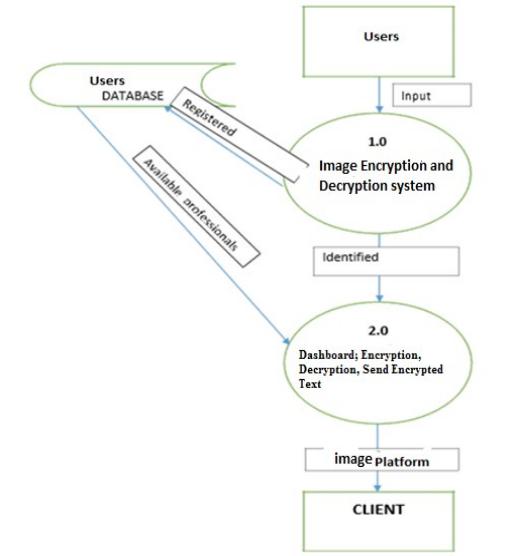

Figure 3: Structure of proposed system

IV. SYSTEM IMPLEMENTATION

System implementation has to deal with the development and deployment of a new system that has been built to solve a particular need. The process of implementation has a lot of activities that precede the eventual deployment of the new system. It starts with coding, site preparation, testing of the system both by the developer and the intending users, debugging, training, cut over strategy specification, system maintenance and system documentation. System implementation describes how the different parts of the system are interacting with each other to give us a feasible software solution. Proper implementation is essential to provide a reliable system to meet organizational requirements and user need.

Below shows the screen shots of the proposed systems.

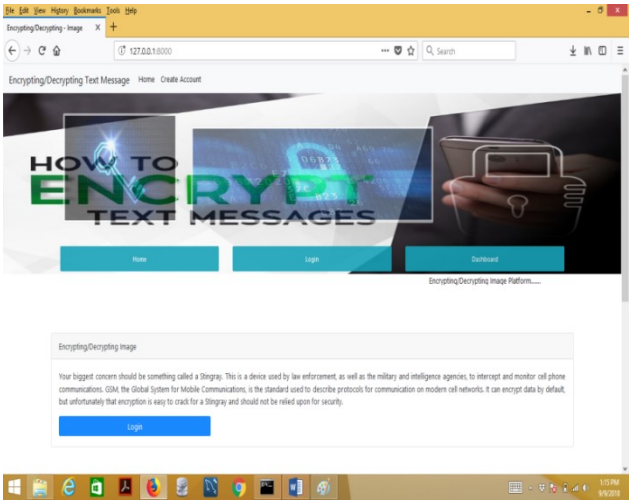

Figure 4.0: input form implementation

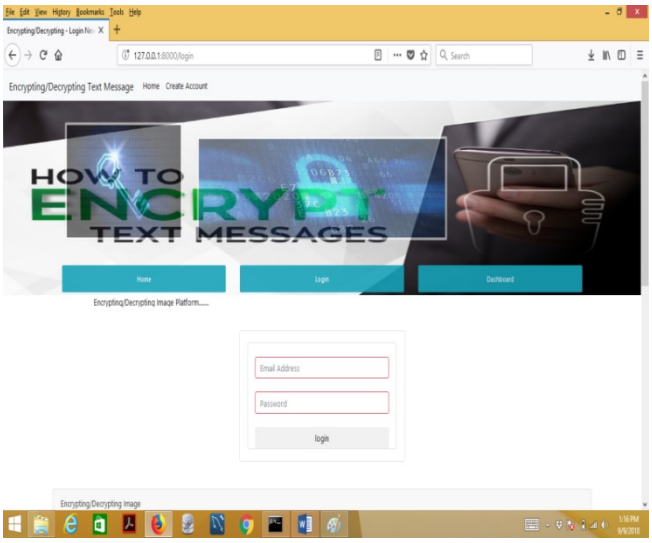

Figure 4.1: Login input form implementation

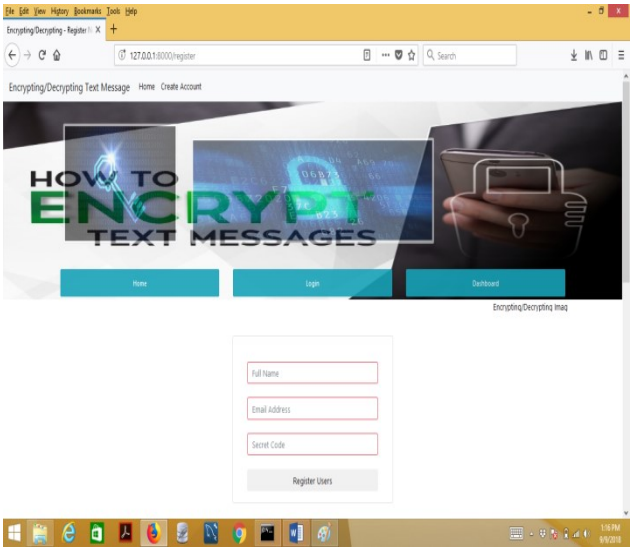

Figure 4.2: Register input form implementation

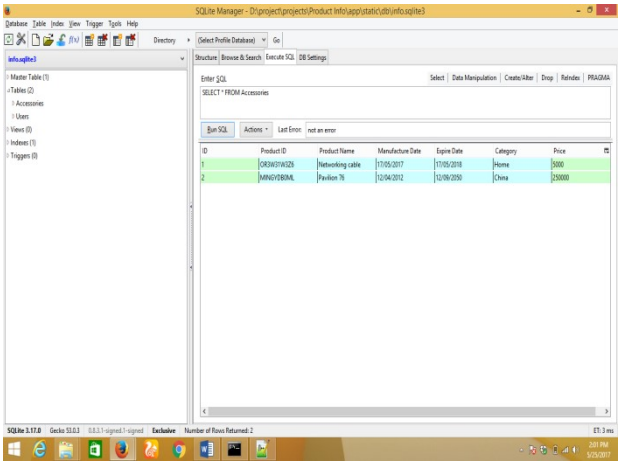

Figure 4.3: Database implementation

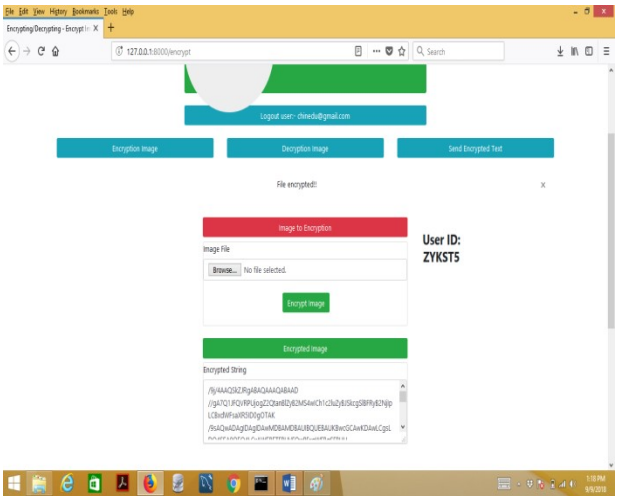

Figure 4.4: Image Encryption (Dashboard)

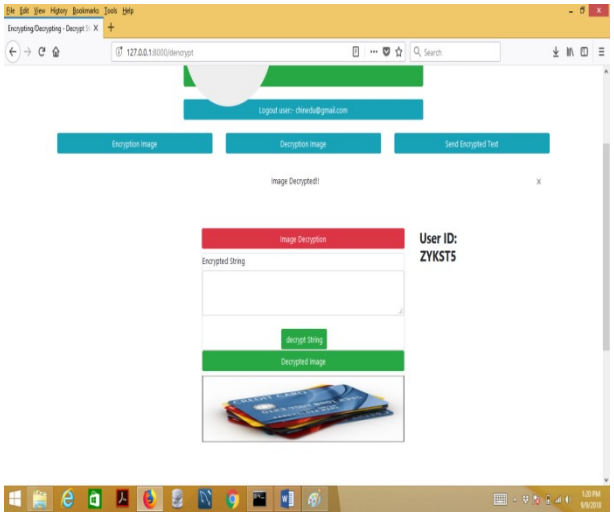

Figure 4.5: Image Decryption

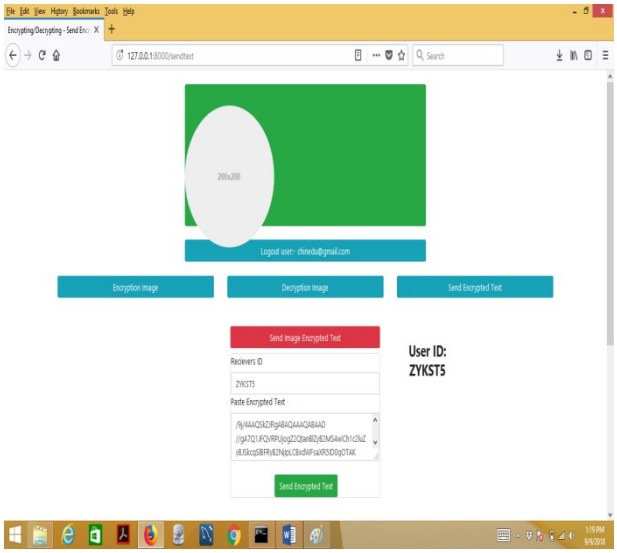

Figure 4.6: Send Encrypted Image

V. RESULT AND DOCUMENTATION

This paper focuses on design and implementation of web based application that runs on browser. Image encryption and decryption platform uses the platform to encrypt into string and send as email to users. This comprises of the documentation of how the system can be used. Below is a step by step procedure for the installation of Python flask, which was used for the development of the system. It also explains how to run the program. In other to install the Python flask, the following steps are to be followed

1. First download Python open source flask framework from here. Setup is around 3 GB.
2. Mount .msi file (if downloaded)
3. Click on executable file to start the installation.
4. Read the license terms and privacy policy and accept them by selecting the checkbox in front of them. Click on "Next" button.
5. Select the features you want to install then click on "INSTALL" button to start the installation. Setup will create system restore point first before installing Flask Dependencies using PHP components.
6. Once it's done, setup will start acquiring the required components to install and will start Installing core features. It will take few minutes to install it. You may require restarting your system (for once ONLY) in between the setup.
7. Once it Finishes the setup, you will see the success screen
8. Click on "Restart Now" button to restart your system. After restarting your system, you are now ready to use your Python flask.
9. Start the server on the command line Python filename.py

VI. CONCLUSION

In conclusion, this paper was tested in using different operating system. It is a cross platform development. It is executed on browser with port 8000 and 127.0.0.1 and on any other system connected to a server through its IP addresses of the serving machine. Use systems encrypt and decrypt image file and sending of files. The image encryption and decryption algorithm is designed and implemented to provide Confidentiality and security in transmission of the image based data as well as in storage. The scheme presented in this paper has a simple implementation module. The proposed encryption algorithm can ensure multiple criteria such as lossless, maximum distortion, maximum performance and maximum speed. The proposed encryption method in this paper has been tested on different format images and showed good results. Future work will be focused on the development of this algorithm to get exactly errors equal to zero.

REFERENCES

[1] Rinki Pakshwar, Vijay Kwmar Trivedi, Vineet Richharia, (2013) "A survey on different image encryption and decryption technique. International journal of computer science and information technology, vol4, Pp 113-116.

[2] Chima Kwar, Jude Larkin, (2019) "Perceptually lossless compression for mastcam multispectral images: A comparative study. Journal of signal and information science and communication (JSIP), Vol 10, issue 4.

[3] Majid Kham, Fawad Masord, A bdullah Alghafis, Muhammed Amin, Syede Iran, Batool Nagvi, (2019) " A novel image encryption techniques using hybride method of discrete dynamical chaotic maps and Brownian motion. Plos one explore.

[4] Abhinar Srivastava, (2012) "A survey report on different techniques of imahes encryption. International journal of emerging technology and advanced engineering, vol 2, issues 6.

[5] Prasithsangaree.P and Krishnamurthy.P, (2003) "Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs," in the Proceedings of the IEEE GLOBECOM, pp. 1445-1449.

[6] Shaojiang Deng, Linhua Zhang, and Di Xiao, (2005) "Image Encryption Scheme Based on Chaotic Neural System", ISNN 2005, LNCS 3497, pp. 868-872.

[7] Huang-Pei Xiao Guo-Ji Zhang, (2006) "An Image Encryption Scheme Based On Chaotic Systems‖". IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, Pp13-16.

[8] Guosheng Gu, Guoqiang Han, (2006) "An Enhanced Chaos Based Image Encryption Algorithm‖". IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06).

[9] NIST Computer Security Division's (CSD) Security Technology Group (STG) (2013). "Block cipher modes". Cryptographic Toolkit. NIST. Retrieved April 12.

[10] Aloha Sinha, Kehar Singh, (2003) "A technique for image encryption using digital signature", Optics Communications, Pp 1-6.

[11] S.S.Maniccam, N.G. Bourbakis, (2001) "Lossless image compression and encryption using SCAN", Pattern Recognition 34, PP 1229-1245.

[12] Jiun-In Guo, Jui-Cheng Yen, "A new mirror-like image encryption algorithm and its VLSI architecture", Department of Electronics Engineering National Lien-Ho College of Technology and Commerce.

[13] Simar Preet Singh, and Raman Mainim. (2011) "Comparison of Data Encryption Algorithms" International Journal of Computer Science and Communication Vol.2, No. 1, pp. 125-127.

[14] Jui-Cheng Yen, Jiun-In Guo, "A new chaotic image encryption algorithm",Department of Electronics Engineering National Lien-Ho College of Technology and Commerce, Miaoli, Taiwan, Republic of China, E-mail: jcyen@mail.lctc.edu.tw