Cloud Authentication Based on Encryption of Digital Image Using Edge Detection

Ali A.Yassin*, Abdullah A. Hussain, Keyan Abdul-Aziz Mutlaq
Computer Science Dept., Education College for Pure Science, Basra University,
Basra, 61004, Iraq,
Email: ali.yassin@uobasrah.edu.iq, aliadel79yassin@gmail.com

***Abstract*—** The security of cloud computing is the most important concerns that may delay its well-known adoption. Authentication is the central part of security in cloud computing model, aiming to guarantee that stored data are permitted to be accessed only by valid/certified users. There are several authentication schemes that based on username/password, but they are considered weak methods of cloud authentication. In the other side, image's digitization becomes highly vulnerable to malicious attacks over cloud computing. In this paper, we propose two-factor authentication scheme based on image partial encryption to overcome above aforementioned issues and drawbacks of authentication schemes. Additionally, we use a fast partial image encryption scheme using Canny's edge detection with symmetric encryption is done as a second factor. In this scheme, the edge pixels of image are encrypted using the stream cipher as it holds most of the image's data and then we applied this way to authenticate valid users. The results of security analysis and experimental results view that the proposed scheme supports an efficient and secure scheme for real-time image encryption and transmission.

Keywords— *Edge Detection; Authentication; Cloud Computing; Service Provider; Password; Image encryption.*

I. INTRODUCTION

Cloud computing has become a promising technology for acquiring computing and storage resources on demand. Cloud allows customers to keep their services highly available with affordable rate: the customers only need to sequestrate the storage service and pay for the exact amount of used storage; users accordingly can have access to this data anytime/anywhere. Unfortunately, in some ways the cloud computing is dominated by the proliferous security threat springing from the many kinds of attacks. As the kernel security element, password authentication plays a constitutional role in modern computing systems [1].

Our work focuses on two topics in security world: the first one is password authentication while the second topic represents encryption of digital image.

A. Password Authentication

The most widespread authentication scheme is textual password. The drawbacks of this scheme like eves dictionary attack; insider attack, dropping, and social engineering are well known. There are some schemes based on generating a random and length password that can make the system more secure. But the main issue is the difficulty of remembering those passwords. In the other side, there are many studies explained that valid users tend to select short passwords that are easy to remember. Unluckily, these passwords suffered from online/off guessing attacks. There are another techniques are graphical passwords and biometrics. Also, these two techniques many disadvantages such as finger prints, DNA, facial recognition that required extra hardware/software. Additionally, these schemes have been presented but not yet widely adopted and the identification process can be slow [2, 3].

B. Image Encryption

Image encryption becomes necessary applications in the Internet communication, medical imaging, database management system, multimedia systems, telemedicine, etc. The security of digital images has gained more attention lately, and several image encryption schemes have been presented to improve the security of images transmission. Image encryption schemes aim to convert digital image to another one that is difficult to understand. On the other side, image decryption restores the original image from the encrypted image. Most of the algorithms exclusively intended to encrypt digital images are proposed in the mid-1990s. Most of these methods are found for a specific image format compressed or uncompressed [4, 5].

C. Our Contributions

In this paper, we propose a new scheme for two-factor password authentication, solving the issues in the ordinary setting. In particular, the motivations of our work are five-fold.

First, our schemes based on two-factor authentication does not require any cost and provides many features such as identity management and session key agreement between valid user and service provider.

Second, we suggest using digital image as a second factor and proposed a new image partial encryption algorithm that based on edge detection feature to encrypt and decrypt image. The purpose is to reduce the time process of second factor and increase the security of our proposed scheme.

Third, we experiment on the common password authentication structure, and the results empirically prove that traditional password authentication has restricted scalability. We also apply a prototype of our proposed scheme, which explains really nice performance.

Fourth, our proposed scheme contains important merits as follows: (1) it provides mutual authentication between user and service provider; (2) it accomplishes user anonymity; (3) The service provider and a user can achieve authenticated session's keys; (4) it allows users to

freely choose their password; (5) it provides revocation phase when the user lost his authentication keys; (6) it describes by low cost, simple integration with available infrastructure, and essay to deploy and manage.

D.Organization

The rest of this paper is organized as follows. The necessary primitives and requirements of our scheme exist in Section 2. An overview of related work is displayed in Section 3. Our proposed scheme is presented in Section 4. We detail the security analysis and implementation results in Section 5, and Section 6 concludes the paper.

II. Main Tools

A. Edge Detection

We can use the edge method to detect edges, which are those places in an image that correspond to object boundaries. To find edges, this method looks for places in the image where the intensity changes rapidly, using one of these two criteria: Places where the first derivative of the intensity is larger in magnitude than some threshold Places where the second derivative of the intensity has a zero crossing edge provides a number of derivative estimators, each of which implements one of the definitions above. For some of these estimators, you can specify whether the operation should be sensitive to horizontal or vertical edges, or both. Edge returns a binary image containing 1's where edges are found and 0's elsewhere. The most powerful edge-detection method that edge provides is the Canny's method. The Canny method differs from the other edge- detection methods in that it uses two different thresholds (to detect strong and weak edges), and includes the weak edges in the output only if they are connected to strong edges. This method is therefore less likely than the others to be "fooled" by noise, and more likely to detect true weak edges. Fig. 2 shows the results of applying Canny edge detectors to Lena image [6-8].

B. Histogram

A histogram image is the mathematical standard of the digital image. Furthermore, it helps to understand the distribution of the graphic image. The histogram image means the process of distribution density of brightness and the contrast in the gray-level image [5, 6]. This method is applied in our approach as measure, any person can note enhanced ratio during this scale.

C. Peak Signal-to-Noise Ratio (PSNR)

The term is an appearance for the ratio between the power of maximum possible signal's value and the power of blemishing noise that actives the quality of its peak signal-to-noise ratio (PSNR) depiction. Because several signals have a very extensive, (ratio between the maximum and minimum are possible values of an irregular quantity). The PSNR is generally expressed in terms of the logarithmic decibel scale. The following equations explain the mathematical representation of PSNR [6-8]:

$$\mathrm{PSNR} = 20\log_{10}\left(\frac{\mathrm{Max_f}}{\sqrt{\mathrm{MSE}}}\right) \qquad (1)$$

$$\mathrm{MSE} = \frac{1}{\mathrm{mn}}\sum_{0}^{\mathrm{m}-1}\sum_{0}^{\mathrm{n}-1}||\mathrm{f(i,j)} - \mathrm{g(i,j)}||^2 \qquad (2)$$

Where:-

MSE: Mean Square Error.
f : Matrix data of our original image.
g : Matrix data of our degraded image in question.
m : The numbers of rows of pixels of the images and i represents the index of row.
n : The number of columns of pixels of the image and j represents the index of column.
Maxf : Maximum signal value that exists in original "known to be good" image.

III. Related Work

A. Image Encryption

Information privacy is an essential feature of digital image encryption. The privacy of the encrypted data with stability in time and cost effectiveness of the encryption method is the main challenge that faced in image encryption topic. There are many related work referred to this challenge [9] distributing via the frequency, spatial, and the hybrid field methods in full encryption schemes.

Saroj et al. [10] propose image encryption scheme using the Hill cipher. They are constructing self-invertible matrix for Hill Cipher scheme. Then, they used this key matrix to encrypt gray level as well as color images. Their scheme works fine for all types of digital images excluding the images with background of the same gray scale or same color. Additionally, their scheme required time processing for full image encryption.

Nien et al. [11] applied a hybrid encryption technique for the true image depended on the multi-chaotic model. They combined the Pixel-Chaotic-Shuffle (PCS) and Bit-Chaotic-Rearrangement (BCR) schemes. The first one (PCS) a fast encryption scheme which can vary the locations of each pixel, is practical to fully disregard the original image outlines applying four third-order chaos's like Henon, Lorenz, Chua and Rössler chaos maps. The second one (BCR) employs chaos scheme to make chaotic codes reorganization in pixels, are practical. The merging of the PCR and the BCR will causes to increase the key space of digital images and suffers from resisting the extensive attack when correlation coefficient is refers to 0.0031.

R. Munir [12] presents a technique that uses the Arnold Cat map transformation on low frequency sub-band of the DCT transformed to encrypt image. Their essential idea for choosing the low frequency sub-band of the DCT transformed image is certified to the truth that the human visual system (HVS) is more figured to important information (such as object, shape) at the lower frequencies compared with the higher frequency information. Their scheme is represented to be strong against noise, though to some amount since the decrypted image views some attendance of noise.

In this paper, we use partial image encryption based one Canny's edge detection as a second factor to authenticate valid user in cloud computing model. TTP sends important information (image, key) to valid user and cloud service provider, respectively. The shared key derives from edge detection of image and uses to encrypts/decrypts image. Additionally, our proposed scheme embeds salt key with shared key to generate one time key for each user's login that leads to generate once. image partial encryption for each authentication phase. In the performance our presented scheme has been evidenced to achieve sturdy security with low cost and high performance compared with previous schemes.

B. Password Authentication

Remote user authentication scheme gains a valid user to access the services and resources existing by the remote system. There are many schemes based on smart card [13-16], and other focused on cloud computing [17, 18]. Most of such scheme, though quite significant and useful, fundamentally supports an incremental advance to the same basic theme. A more secure scheme is the two-factor authentication that does not only verify the username/password pair, but also needs a second factor such as a token device, biometric. However, the feasibility of second-factor authentication is limited by the deployment complexity, high cost and the cloud security is compromised when the token is missing or purloined. Furthermore, these schemes are failed to resist well-known attacks such as replay attacks, reflection attacks.

Our proposed scheme overcomes above aforementioned issues and based on two-factor authentication, the first one anonymous password while the second factor based on partial image encryption for generating a strong scheme which have a good balance between security and performance in cloud environment. Table 1 describes a comparison of security properties.

IV. Our Proposed Scheme

The common notations in Table 2 will be used throughout this paper. Our proposed scheme consists of three phases— setup, registration, and authentication. In the setup phase, the main components (TTP, SP, U_i) also uses a cryptographic hash function $h(.)$, A symmetric key encryption/decryption $Enc(.)/Dec(.)$, TTP sets up $n = p * q$; where both p and q are two large primes. The user (U_i) sends his username $(Un_i = h(username))$ and password $(pw_i = h(password))$ to the trusted third parity (TTP) through a secure channel. However, the proposed scheme prevents TTP to perceive the real username/ password of each valid user. As a result, TTP cannot impersonate the user to login system. After that, TTP stores (Un_i, pw_i), generates digital image (img_i), then provides public parameters keys $PK = (Un_i, pw_i, img_i, sh)$ and a secret keys $SK = (img_i, sh, n)$ to service provider and each user, respectively, in the secure channel.

So, TTP generates shared key sh by popping the value of gray-scale image's pixels which posited at edge detection of image (img_i). Fig. 1 demonstrates the mechanism of computing a shared key (sh). Lastly, U_i encrypts his secret keys $(SK' = Enc_{pw}(SK))$ by using his password and then saves his encrypted file at his preferred storage such as USB, Samsung mobile. After registration phase, the user can use his secret key to enter authentication phase to login. The 2FA authentication session is qualified as follows (see Fig. 2).

Table 1. Comparative Analysis of Authentication Schemes

Features	Our Proposed Scheme	[13]	[14]	[15]	[16]	[17]
Identity Management	Yes	Yes	Yes	Yes	Yes	Yes
User Privacy	Yes	Yes	Yes	Yes	Yes	Yes
Mutual Authentication	Yes	No	Yes	Yes	Yes	Yes
Session Key Agreement	Yes	No	No	Yes	Yes	No
User anonymity	Yes	Yes	No	Yes	No	No
Replay Attack	Yes	No	No	No	No	No
Impersonation Attack	Yes	No	No	Yes	No	No
No extra software and hardware	Yes	No	No	Yes	No	No

Table 2. Notations of our proposed scheme

Symbol	Definition
$h(.)$	A cryptographic hash function.
$Enc(.)$ $/Dec(.)$	A symmetric key encryption/decryption function.
n, p, q	Large primes numbers.
Un_i, Un_i'	User anonymity.
pw_i	Password anonymity.
sh	Shared key derives from edge detection of image (img_i).
PK	Public parameters provided by TTP to SP at setup phase.
SK	Secrete keys provided by TTP to U_i at setup phase.
pw_i'	One time password anonymity.
r_i, SK', K_i	Other miscellaneous values which are used in the verification
p_i	A random pixel selects from image.
(x, y)	The positions (x, y) of pixel (x, y).
Edge	Cany edge detection function.

1. $U_i \rightarrow SP: Un_i', pw_i', r_i$. U_i performs the following steps:
   - Decrypt his secret keys file based on his password $SK = Dec_{pw}(SK')$.
   - Generate random number $r_i \in Z_n^*$ and compute one time anonymous username $(Un_i' = h(username)$ and password $(pw_i' = h(h(password)||sh||r_i))$.

- Send Un_i', pw_i', r_i to SP as a first factor.

2. SP $\rightarrow U_i: (x, y), p_i$. SP checks the validity of user's first factor as follows:
   - Compute $pw_i'' = h(pw_i||sh||r_i)$ and check whether pw_i'' equals the stored pw_i'. If so, he accepts the user's first-factor authentication request and performs the next step. Otherwise, SP terminates login phase.
   - SP generates a random number from image ($p_i \in img_i$) and positions (x, y) of p_i as a challenge to valid user for ensuring from validity of SP.
3. $U_i \rightarrow$ SP: E'. User verifies $img_i(x, y) ?= p_i$. If it holds, then U_i ensures from validity of SP and computes second factor based on computing edge detection of his image ($Eimg_i = Edge(img_i)$) and secret key ($K_i = sh \oplus p_i$) for each user's login request, respectively. Then, the user encrypts edge detection image $E' = Enc_{K_i}(Eimg_i)$. Finally, he sends both E' and K_i to SP.
4. SP. Upon receiving the second factor in Step 3. SP computes $K_i' = sh \oplus p_i$, he can authenticate the user by comparing $Enc_{K_i'}(Edge(img_i))$ with E' in securely manner. If so, SP accepts the user's login request. Otherwise, he rejects the login phase.

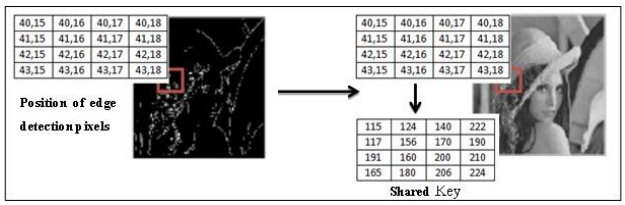

Fig. 1. The mechanism of computing shared key

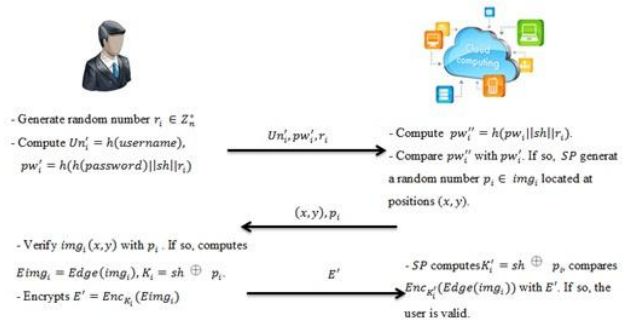

Fig 2. The mutual authentication phase of our proposed scheme

V. Experimental Results

A. Security Analysis

Theorem 1. Our proposed scheme can supply mutual authentication.

Proof. The mutual authentication feature requires that an attacker cannot impersonate a legal user to the service provider, and vice versa. Only the valid user has the secret factors (Un_i', pw_i', r_i, E') to send these factors to the service provider. SP compares (Un_i', pw_i') and E' with (Un_i', pw_i'') and $Enc_{K_i'}(Edge(img_i))$, respectively. If so, a user is authenticated. To complete mutual authentication, the user verifies $img_i(x, y)$ with p_i. If it holds, then U_i ensures from validity of SP.

Theorem 2. Our proposed scheme can supply user's password anonymity.

Proof. If an adversary attempts to eavesdrop on the user's login request, he cannot find the user's password anonymity from crypto hash function $pw_i' = h(h(password)||sh||r_i)$ since it is embedded each of shared key sh and a random number r_i, which are not identified to an adversary. Additionally, r_i generates once for each user's login request. So, it has been encrypted by shared key sh existed just in U_i and SP. Hence, it is difficult for an adversary to disclose the user's password.

Theorem 3. Our proposed scheme can provide security of the stored data.

Proof. The proposed scheme, only user's secret key (SK) is stored on user's storage such as USB, mobile phone. The data of SK does not help an adversary to use it without the user's password. If the legal user loses his prefer storage, it is difficult for any adversary to access or update the credential information because he cannot obtain the user's secret key (SK).

Theorem 4. The proposed scheme can support Known-key security and session key agreement.

Proof. In our proposed scheme, when the user sends the second factor to login the server, he generates secret key $K_i = sh \oplus p_i$) to encrypt edge detection of his image which represents his second factor $E' = Enc_{K_i}(Eimg_i)$. Even if an adversary can access to the previous session key, he is still unable to get fresh values of K_i which generates once time for each user's login session. So an adversary cannot compute the new session key. Continuously, the service provider can obtain the same new key K_i' based on secret parameters (sh,p_i) to compute $Enc_{K_i'}(Edge(img_i))$. Finally, SP checks the validity of second factor based on K_i'. Additionally, our proposed scheme depends on digital image to obtain secret keys (K_i, K_i') that derived by using $((x, y), p_i)$.

Theorem 5. Our proposed scheme can forward Secrecy.

Proof. Our proposed scheme preserves of the password even when the secret key K_i is disclosed or leaked. If the secret key K_i is revealed by the adversary, the authentication of the system is not impressed, and he cannot use this key in the next login phase. At the same time, it is extremely hard that an adversary can derive the secret key which consists of random number that derives from image ($p_i \in img_i$) and shared key sh. An adversary still cannot obtain the secret key K_i which used to encrypt second factor $E' = Enc_{K_i}(Eimg_i)$.

Theorem 6. Our proposed scheme can resist the MITM Seed-tracing attack and off-line guessing attack.

Proof. Often, OTP token schemes are suffered from the fixed seed-key. In the moment, scheme generated a fixed pseudo random series style. An adversary may possess the opportunity to hunt the seed-key if he obtains enough sequences of OTP values from the same token. This type

attack is called MITM Seed-tracing attack. Furthermore, the user may be threatening by Shoulder-surfing attack. This attack may be happened while the user is entering the password via the login phase or using the OTP token. The adversary can get user's secretive information during the secret attack without user knowing anything. Then, he can trace out Seed-key, if he gets enough sequences of OTP codes. Our proposed scheme resists this type of attacks. The adversary does not gain any advantages from his attempts to detecting seed password; it cannot obtain the values of $(\mathrm{sh}, \mathrm{img_i}, \mathrm{Eimg_i}, \mathrm{K_i})$ to perform its malicious attack. The adversary must perform the following operations to get the seed of password.

- He must guess the values of $(\mathrm{sh}, \mathrm{img_i}, \mathrm{Eimg_i}, \mathrm{K_i})$.
- The adversary cannot access to secure credential file that saves in extra-device by user or even the adversary comprises the service provider; He cannot get user's password to decrypt user's credential file (SK).

Theorem 7. Our proposed scheme can provide revocation.

Proof. In case of lost or stolen of user's prefer storage such as USB, $\mathrm{U_i}$ will present request to SP for its revocation by pushing his first factor $(\mathrm{Un_i'}, \mathrm{pw_i'})$. SP verifies the first factor and ensures whether $\mathrm{pw_i'} = \mathrm{pw_i''}$. If the result is valid, SP deletes registration user's file $(\mathrm{SK} = (\mathrm{img_i}, \mathrm{sh}, \mathrm{n})$ from registration table. Lastly, the user can change his username and password by re-performing the registration phase. Additionally, an adversary cannot get any benefits from stealing user's extra storage because he cannot be tolerated to decrypt registration user's file which requires from an adversary to obtain user's password $\mathrm{pw_i}$.

B. Implementation and Results

In this section, we conduct several experiments for gauging the efficiency and the effectiveness of our work. Fig. 3 shows time processing of mutual authentication phase, first factor, and second factor. However, the average time for the login and authentication phase of our work is equal to 0.136141 seconds for each user who indicates the high speed of our solution. Furthermore, the time processing of first factor and second factor are 0.00054 and 0.135061, respectively. The estimation parameters are declared in Table 3. The time requirement of our scheme is brief in Table 4. We test the effectiveness in terms of authentication accuracy. We have registered during our experiments 2500 users and suppose that each user needs maximum 0.75 second for logging the system.

In image encryption for the second factor, we demonstrate the experimental results of the first two users' images of different sizes with gray-scale (0-255). The results of experimental and statistical analysis view that our proposed scheme supports an efficient and secure manner for real-time image encryption and transmission. Figures (4, 5) explain histogram of original, encrypted, and decrypted images. Addition to that, table 5 shows the results of PSNR and entropy of original, encrypted, and decrypted images.

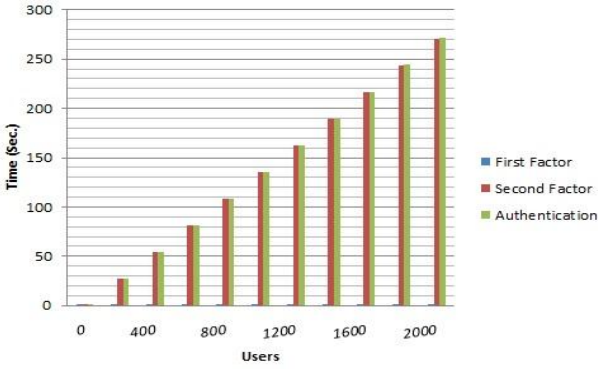

Fig 3. shows the performance of our proposed scheme

Table 3. Estimation Parameters.

Symbol	Definition
T_h	Time processing of a hash function.
T_{Xor}	Time processing of Xor function.
T_{Opr}	Time processing of mathematical operations such as multiplication, addition and subtraction.
T_{Enc}	Time processing of symmetric encryption operation.
T_{Dec}	Time processing of symmetric decryption operation.
$T_{\|\|}$	Time processing of concatenation function.
T_{Edge}	Time processing of Canny's edge detection function.

Table 4. Performance of our proposed scheme.

Phase	**TTP**	**User**	**Service Provider**
Setup & Registration	$2T_h + T_{Opr}$	T_{Enc}	--
Login	-------	$3T_h + T_{Opr} + T_{Dec} + 2T_{\|\|}$	--
Mutual Authentication	-------	$2\,T_{Opr} + T_{Enc} + T_{Edge} + T_{Xor}$	$2\,T_{Opr} + T_{Enc} + T_{Edge} + T_{Xor} + T_h + 2T_{\|\|}$
Total	$2T_h + T_{Opr}$	$3\,T_{Opr} + 2T_{Enc} + T_{Edge} + T_{Xor} + 3T_h + 2T_{\|\|}$	$2\,T_{Opr} + T_{Enc} + T_{Edge} + T_{Xor} + T_h + 2T_{\|\|}$

Table 5. PSNR and Entropy of encrypted/decrypted image

Original image	**PSNR of encryption image**	**Entropy of encryption image**	**Entropy of decryption image**
Edge of Boy's image	6.0458	7.9971	0.5075
Edge of House's image	7.3631	7.9969	0.5825

VI. CONCLUSION

In this paper, we have proposed a newer authentication scheme for cloud computing environment that includes one-time password's anonymity as a first factor and partial image encryption based on edge detection as a second factor. Our proposed scheme aims to support more functionality and to resist familiar attacks. These vital merits include (1) the valid user can freely choose his passwords; (2) our proposed scheme supports mutual authentication between service provider and legal user; (3) it achieves one-time password anonymity; (4) Service provider and legal user can produce authenticated sessions keys; (5) our proposed scheme can provide revocation and security of the stored data. Moreover, our scheme can resist MITM Seed-tracing attacks, the stolen-verifier problem, off-line guessing attacks, reflection attacks, replay attacks, forgery attacks, and parallel session attacks. In the other side, we proposed a fast image encryption scheme for images using Canny's edge detection. In performance evaluation, our scheme has been proven to obtain strong security with lower communion cost than previous works.

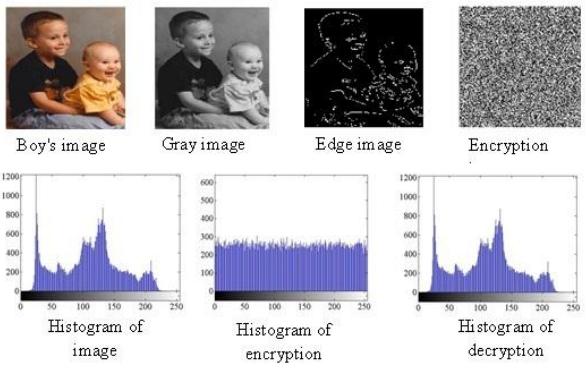

Fig.4 shows the main stages of encryption/decryption of Boy's image

REFERENCES

[1] S. Subashini and V. Kavitha, "A survey on security issues in service delivery models of cloud computing", Journal of Network and Computer Applications, Vol.34, No.1, Jan. 2011, pp.1-11.

[2] S. Shin, K. Kobara, and H. Imai, "A Secure Construction for Threshold Anonymous Password-Authenticated Key Exchange", IEICE Transactions on Fundamentals, Vol.E91-A, No.11, 2008, pp.3312-3323.

[3] J. Katz, M. Yung, "Scalable protocols for authenticated group key exchange". Journal of Cryptology 2007; Vol. 20, No.1, pp.85–113.

[4] R. Kaur, and E. K. Singh, "Image Encryption Techniques : A Selected Review", Journal of Computer Engineering (IOSR-JCE), Vol. 9, No. 6, 2013, pp. 80–83.

[5] E. Thambiraja, G. Ramesh, and Dr.R.Umarani, "A Survey on Various Most Common Encryption Techniques",

[6] International Journal of Advanced Research in Computer Science and Software Engineering, vol. 2, no. 7, July 2012, pp. 226–233.

[7] K. Lebart, C. Smith, E. Trucco, and D. M. Lane, "Automatic indexing of underwater survey video: algorithm and benchmarking method," IEEE J. Ocean. Eng.", Vol. 28, No. 4, 2003, pp. 673–686.

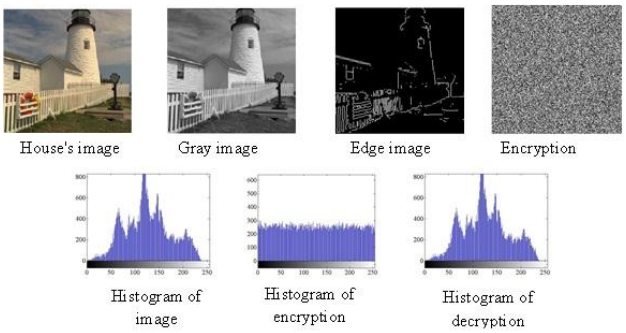

Fig.5 shows the main stages of encryption/decryption of house's image

[8] Ali A. Yassin, Rana M. Ghadban, Salah F. Saleh, Hikmat Z. Neima, "Using Discrete Wavelet Transformation To Enhance Underwater Image", International Journal of Computer Science Issues, Vol. 10, No. 2, pp. 220-228, 2013.

[9] I. Vasilescu, C. Detwiler, and D. Rus, "Color-accurate underwater imaging using perceptual adaptive illumination", Autonomous Robots , Vol.31, No. 2-3, 2011, pp. 285-296.

[10] R. Rhouma, D. Arroyo, and S. Belghith, "A new color image cryptosystem based on a piecewise linear chaotic map", in 6th International Multi-Conference on Systems, Signals and Devices, Mar. 2009, pp. 1–6.

[11] S. K. Panigrahy, B. Acharya, and D. Jen, "Image Encryption Using Self-Invertible Key Matrix of Hill Cipher Algorithm", 1st International Conference on Advances in Computing, Chikhli, India, February 2008.

[12] H. H. Nien, W. T. Huang, C. M. Hung, S. C. Chen, S. Y. Wu, C. K. Huang, and Y. H. Hsu, "Hybrid image encryption using multi-chaos-system", in 7th International Conference on Information, Communications and Signal Processing (ICICS), Dec. 2009, pp. 1–5.

[13] R. Munir, "Robustness Analysis of Selective Image Encryption Algorithm Based on Arnold Cat Map Permutation", in Proceedings of 3rd Makassar International Conference on Electrical Engineering and Informatics, Nov. 2012, pp. 1–5.

[14] M. L. Das, A.Saxena, and V. P. Gulati, "A dynamic ID-based remote user authentication scheme", IEEE Transactions on Consumer Electronics, Vol.50, No. 2, pp.629-631, 2004.

[15] H. Y. Chien, J. K. Jan, and Y. M Tseng, "An efficient and practical solution to remote authentication: smart card", J. of Computers and Security, Vol.21, No. 4, pp.372-375, 2002.

[16] Ali A. Yassin , Hai Jin Ibrahim A., Weizhong Qiang , Deqing Zou , "A Practical Privacy-preserving Password Authentication Scheme for Cloud Computing," Parallel and Distributed Processing Symposium Workshops & PhD Forum (IPDPSW), 2012 IEEE 26th International, vol. , 21-25 May 2012, pp. 1210-1217.

[17] A J Kumar Choudhury, P. Sain , M. Hyotaek, Lim Hoon Jae-Lee , "A Strong User Authentication Framework for Cloud Computing," Services Computing Conference (APSCC), 2011 IEEE Asia Pacific , 12-15 Dec 2011 , pp. 110-115.

[18] K. Venkataramana , Dr M Padmavathamma, "Agent Based approach for Authentication in Cloud", IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), vol. 2, No 3, pp. 598-603, June 2012