Securing Images in Cloud using Hyper Chaos with User Authentication

Shaheen Ayyub
Research Scholar
Department of Computer Science & Engg.
MANIT, Bhopal, India

Praveen Kaushik
Asstt. Professor
Department of Computer Science & Engg.
MANIT, Bhopal, India

ABSTRACT
Security in the cloud is the top most concern. To achieve trust and preserve the privacy of data stored in third-party cloud storage has emerged as a key research area. To achieve this, several different techniques have been proposed based on cryptography. Secret sharing schemes and chaos based encryption have also been considered to address these issues of trust and privacy by various researchers. In this paper, we are proposing a new scheme to encrypt the private and sensitive images of users in the third party storage named as "Securing images in cloud using hyper chaos with user authentication" to solve the problem of authenticating users. Chaos based encryption with image captcha authentication using VCS is a major advantage of this scheme. Chaos based encryption is a very secure method for encryption. Many researchers have used the above technique but user authentication or authorization is not mentioned in their schemes. To increase more security we have included the authentication in the scheme. In this paper the authentication process is explored in depth and only the overview of encryption process is given. For securing the authentication logistic map is used to divide and shuffle the original image captcha into many blocks. The use of visual cryptography technique is explored to preserve the privacy of image captcha. Part of the image share will be kept with the image owner such that the original image captcha can be revealed only when both (user, owner) of the shares are simultaneously available. The individual share images do not reveal the identity of the original image captcha. Once the original image captcha is revealed after merging different shares, the user will be considered as authenticated user. Then only the encrypted key for the images will be transferred to the user. Dynamically generating the Captcha image by the system is one of the major advantage of the system.

Keywords
Cloud security, Images, Visual cryptography, Captcha, Logistic map

1. INTRODUCTION
Cloud computing is a technology invention which provides the resources like Server, Storage, OS and Network to user on demand service. Cloud computing has emerged as a popular solution to provide cheap and easy access to externalized IT (Information Technology) resources. An increasing number of organizations (e.g., research centers, enterprises) benefit from Cloud computing to host their applications [1]-[2]. Virtualization is the core concept supported in the cloud computing. Resources are provided to cloud users as virtualized manner [3]. Virtualization and cloud computing can be used quite successfully to improve the resilience of an IT environment. Because, they provide the means to recover quickly from component or system malfunctions using failover. Back up of essential applications and data can be quickly taken up. Virtual machines can be migrated from one physical server to another in a live migration; virtual machine images can be restarted in a different location to provide for disaster recovery [4]. There are three types of services in the Cloud. They are Software as a service (SaaS), Platform as a service (PaaS) and Infrastructure as a service (IaaS). Different cloud providers like Amazon, Google, Microsoft, IBM and etc, provide different Cloud services. Based on their requirement the users can utilize these services (SaaS, PaaS and IaaS). By using these three services, users store their data in the cloud storage. User's data is maintained by the cloud providers in cloud environment. The data in the provider's hands could make security and privacy issue in cloud storage because users lose their control over their data. Nothing inside the cloud is visible to the user. So cloud users have to think about their data [5]. Like: how much secure the data in the cloud, Access control and authentication of the cloud. Cloud computing companies say that data is secure, but it is too early to be completely sure of. Only time will tell if users' data is se cure in the cloud. Cloud security and privacy concerns are arising in which both customer's data and application are residing in provider's premises. Security and privacy are always big issue in cloud computing [6]-[7] as shown in Fig.1. It shows the survey report of International Data Corporation (IDC). From the figure, it is clear that security is the top most concern in cloud computing survey.

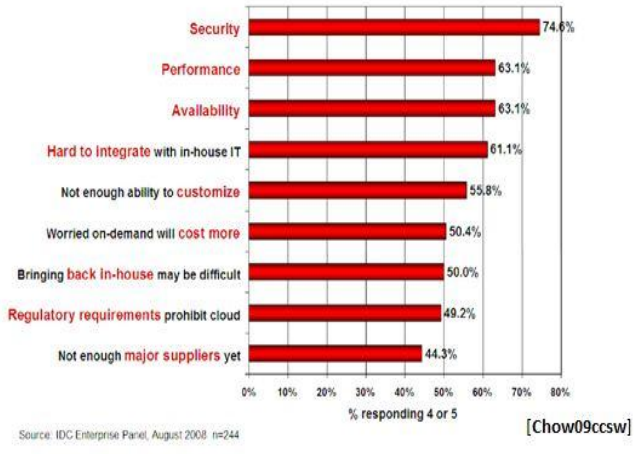

Figure1: Security is a big issue in cloud computing [6]-[7]

There can be two types of attacks in cloud one is insider attack another is outsider attack. Insider as an administrator can have the possibility to hack the user's data. Insider attack is very difficult to be identified. So the users should be very

careful while storing their data in cloud storage. Even though the data is accessed by the third party, they shouldn't get the actual data. So, all the data must be encrypted before it is transmitted to the cloud storage. Although encryption is a prevalent method of securing transmitted data, the data in the encrypted form (*i.e.*, cipher text) will impede operations that are usually conducted on the plaintexts. In order to further process cipher texts and obtain the corresponding results in the plaintext domain, some studies have been devoted to several aspects of encrypted domain operations. Security is also an important issue in communication and storage of images, and as we know encryption is one of the ways to ensure security. Image encryption has applications in internet communication, multimedia systems, medical imaging, telemedicine, military communication, etc. Images are different from text. Only recently, secure text document search in the encrypted domain [8], [9] has been extended to secure multimedia data search [10], [11]. Although traditional cryptosystems may be used to encrypt images directly, it is not a good idea for two reasons. One is that the image size is much greater than that of text. Therefore, encryption time increases in traditional cryptosystems to directly encrypt the image data. Another problem is that in text documents the decrypted text must be equal to the original text. However, this is not the necessity for image data. A decrypted image containing small distortion is usually acceptable due to the characteristic of human perception. Various encryption schemes have been proposed in this regard in the past years. In this paper we have proposed a new scheme for image encryption with user authentication for enhancing the security and privacy of images before storing them on the cloud. In the proposed scheme image captcha based authentication is done. We have used visual cryptography for verifying the image captcha while enhancing the security and for encrypting the images hyper chaos are used while masking is done using flicker images. Visual Cryptography (VC) is a method of encrypting a secret image into shares, such that stacking a sufficient number of shares reveals the secret image. In this paper we have explained the authentication procedure in detail and the short overview of the encryption algorithm.
The rest of this paper is organized as follows. Related work is explained in Section 2. In Section 3, we describe the proposed System framework. In Section 4 proposed scheme is there. Section 5 contains a threat analysis and results of the proposed scheme for some experiments. Section 6 is the conclusion.

2. RELATED WORK

Several researchers have used traditional cryptographic primitives to protect images before storing them in untrusted storage [12][13] which do not admit computation in clouds. Due to the processing overhead resulting from the large data size of digital images and the high correlation among pixels, traditional encryption algorithms, such as DES, AES and RSA, are found to be inefficient for image encryption [14-16]. Comparing with conventional algorithms, chaos based ones have suggested more secure and fast encryption methods [17].

Chaotic maps are sensitive to their initial conditions. A simple change in one pixel of input image affects large number of pixels in the cipher image which makes the computation on cipher image impossible. Chaotic maps have been explored by researchers for image encryption [17]. Arash Nourian *et al* [18] have proposed an algorithm for color image encryption in cloud using cat map. They have used the flicker image to encrypt the original images. Their algorithm is not secure enough to chosen plain text attack. In the algorithms described above they haven't explained about the key transfer mechanism as well as in the above describe algorithm user authentication is also not considered.

Visual cryptography schemes were independently introduced by Shamir [19] and Blakley [20], their original motivation was to safeguard cryptographic keys from loss. These schemes also have been widely employed in the construction of several types of cryptographic protocols [21] and consequently, they have many applications in different areas such as access control, opening a bank vault, opening a safety deposit box, or even launching of missiles.

3. VISUAL CRYPTOGRAPHY

Visual Cryptography is a cryptographic technique in which encryption of visual information is done such that decryption can be performed using the human visual system. It can be achieved by one of the following sharing schemes.

1. (2, 2) Threshold VCS scheme- This is the simplest threshold scheme in which a secret image is encrypted in two different shares that reveal the secret image when they are stacked together. No additional information is required to create this kind of access structure.

2. (2, n) Threshold VCS scheme- In this scheme a secret image is encrypted into n number of shares such that when any two (or more) of the shares are overlaid the secret image is revealed. The user will be prompted for n, the number of participants.

3. (n, n) Threshold VCS scheme-This scheme encrypts the secret image to n shares such that when all n of the shares are combined then only the secret image will be revealed. The user will be prompted for n, the number of participants.

4.(k, n) Threshold VCS scheme- This scheme divides the secret image into n shares such that when any group of at least k shares are combined the secret image will be revealed. The user will be prompted for k, the threshold, and n, the number of participants.

In the case of (2, 2) VCS, each pixel P in the original image is encrypted into two sub pixels called shares. Fig.2 denotes the shares of a white pixel and a black pixel. The choice of shares for a white and black pixel is randomly determined i.e. there is two choices available for each pixel. No share provides any clue about the original pixel since different pixels in the secret image will be encrypted using independent random choices. When the two shares are superimposed, the value of the original pixel P can be determined. If P is a black pixel, we get two black sub pixels; if it is a white pixel, we get one black sub pixel and one white sub pixel.

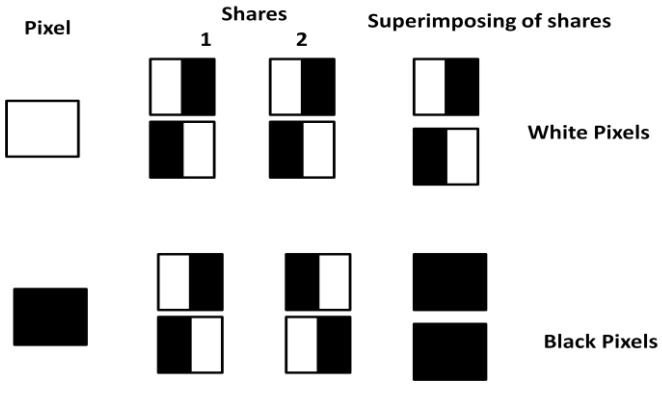

Figure2: (2,2) VC scheme

4. PROPOSED SYSTEM FRAMEWORK

In the proposed scheme, an image owner connects to the cloud and desires to use cloud storage capacity and computational power to store the images securely which can be retrieved or accessed by the cloud user or image owner afterwards. The image owner has a collection of his sensitive image and wants to securely store them on to the cloud. The security enhancing process which is performed in image owner's machine uses images obtained from social media sites such as flicker to create masks for the original image with a lightweight encryption scheme to further enhance the security of the image. The identity of the masks (i.e. Flk_ID) and the keys used for encryption process are kept secret. The image owner creates the key matrix of the keys and ID of the masks used for encryption. Then the key matrix encryption is performed by the image owner. This is done by key transfer mechanism. In which λ-values and λ-vectors are created. λ – vectors are sent to the authorized cloud user. When a cloud user wants to retrieve the image, he extracts the keys and creates the index for searching the remotely stored image collection, and then sends the index to the cloud server.

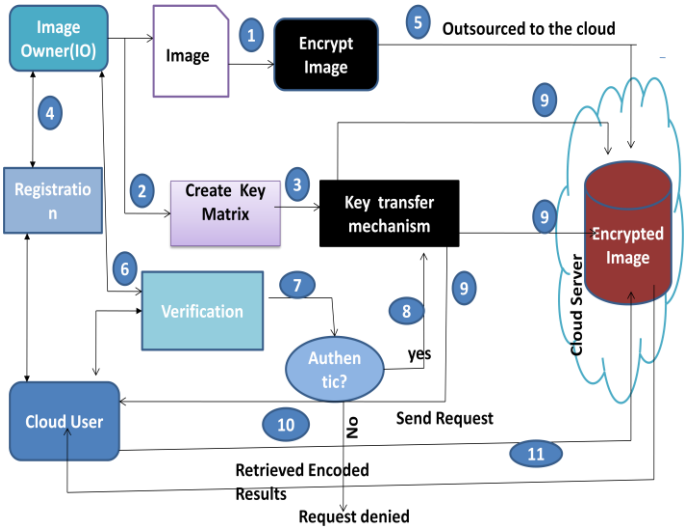

Figure3: System Frame Work

The cloud performs the requested computation on the encrypted images and returns the results in the encoded forms to the cloud user. The cloud user decodes the received results to get the images on which the requested computations are done by the cloud. In this scheme only authenticated user/image owner can retrieve the images. Here user authentication is done by visual cryptography based image captcha. In which the image string is divided into two shares. Share1 with the original image string is kept with the owner and the share2 is sent to the user. Fig.3 shows the basic structure of proposed scheme.

5. PROPOSED SCHEME

The scheme consists of the following steps:

5.1 Image Encryption

A new image encryption scheme with key encryption and user authentication is suggested in this paper, different from others have proposed so far. The original color image is first XORed with the image obtained from the social media (Flicker) by using the flicker ID. Secure hash functions [3] have been used in this scheme as h_1 (z) and h_2(x, y, z), to create the flicker ID, which depends upon the features of the original image. By doing this we apply first complexity to our encryption scheme that makes it more robust against widespread attacks. After hiding the image with the mask hyper chaos [4] and logistic map [5] are applied to shuffle the image and finally encode the image. We have used 4^{th} order RK method to solve the two chaotic systems.

5.2 User Authentication

In this process cloud user is authenticated for retrieving the specific images. This process consists of two phases: one is Registration and the other one is Verification.

5.2.1 Registration

In registration phase the user gets registered for retrieving images. In this the user who wants to register enters a string from his/her side. After getting the string from user's side the owner enters another string from his/her side. Both of the two strings are then concatenated to generate an image captcha. This image captcha is then encrypted by using logistic map and then (2, 2) VC scheme is applied.

5.2.1.1 Image Captcha

A CAPTCHA is a type of test used in computing to determine whether or not the user is a human. The term was given in 2003 by Luis von Ahn, Manuel Blum, Nicholas J. Hopper, and John Langford [22]. The most common type of CAPTCHA was first invented in 1997 by Mark D. Lillibridge, Martin Abadi, Krishna Bharat, and Andrei Z. Broder. This form of CAPTCHA requires that the user type the letters of a distorted image, sometimes with the addition of an obscured sequence of letters or digits that appears on the screen. Because the test is administered by a computer, in contrast to the standard Turing test that is administered by a human, a CAPTCHA is sometimes described as a reverse Turing test. This term is ambiguous because it could also mean a Turing test in which the participants are both attempting to prove they are the computer. In this scheme the user enters a key string for the registration purpose. For the sake of security the key string can be a combination of numbers and alphabets. After getting the string from the user, a random string is generated at the owner side. Both of the two strings are then concatenated and an image captcha is generated [23]. Then image captcha is further processed using logistic map.

5.2.1.2 Logistic Map

After getting image captcha, this image is divided into M×N blocks where M and N are the dimensions of the generated image. These blocks are then shuffled using the following logistic map. For this we create a pseudo random array from the logistic map and disorder the actual arrangements of the blocks.

$$x_{n+1} = r^* x_n(1 - x_n) \qquad (1)$$

For a given x_0 some iteration is performed and a new x_0 is obtained and then random array is created as follows:

$$\text{Random array} = [\text{mod}(x_0 \times 10^{14}, (M \times N\text{-}1))] + 1 \qquad (2)$$

Continuously iterate the logistic map and perform (2) until M×N different values which are all between 1 and M×N are not obtained. This kind of procedure will make the encryption operation more confusing and complex as it adds an extra step to the encryption process, and furthermore the length of the

key will become longer. This process can be more understood from Fig. 3 in which the procedure for 8 blocks is shown. As shown in Fig. 4, the initial image blocks become totally disordered using the random permutations. The disordered image is obtained as follows. First, the block number "1" is changed with block number "6." Next, the block number "2" is changed with block number "8." Then the block number "3" is changed with block number "7" and the block number "4" is changed with block number "2." Then block number 5, 6, 7 & 8 are changed with block number 5, 4, 1 &3 respectively. Doing this procedure, we apply another complexity to our encryption scheme that makes it more robust against widespread attacks.

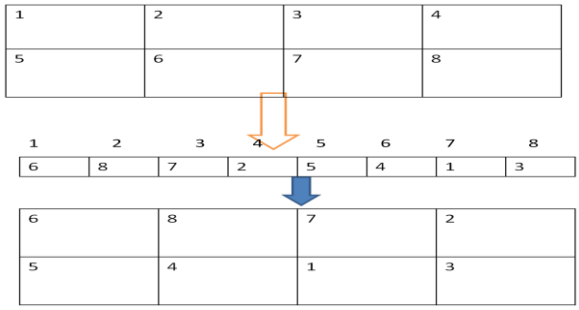

Figure 4: Shuffling of blocks

5.2.1.3 Visual Cryptography

After shuffling the image captcha the resulted image is divided into 2 shares by using (2,2) VCS such that the image is divided according to black and white pixels. One of the shares is kept with the user and the other share with the original image captcha is kept with the owner. The registration process is shown in fig. 5(a).

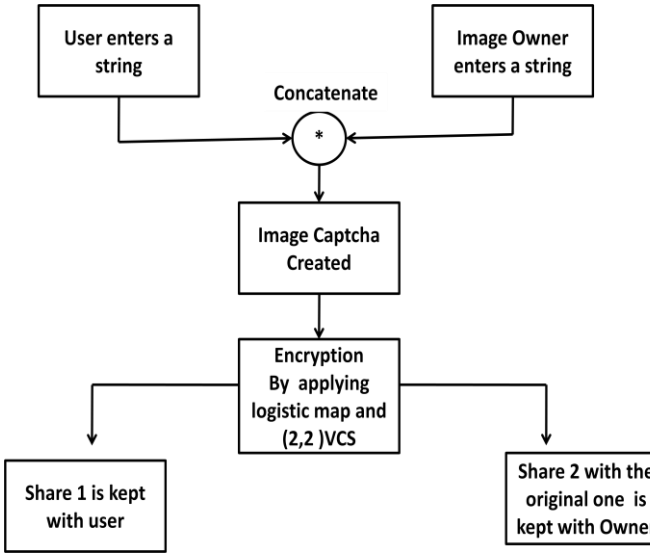

Figure 5(a): Registration

5.2.2 Verification

When user wants to be authenticated for retrieving/accessing the image, he is asked to enter t his share which is kept with him. Then the owner retrieves the share which is stored in the database, related with the information of a particular user. Both of the two shares are stacked together to produce the image captcha. The generated image captcha is then matched with the original image captcha. If a matched is found then the user is authenticated for the image otherwise his request is denied. Verification process is depicted in fig. 5(b). The encryption process with the shuffling using logistic map is shown in fig 6.

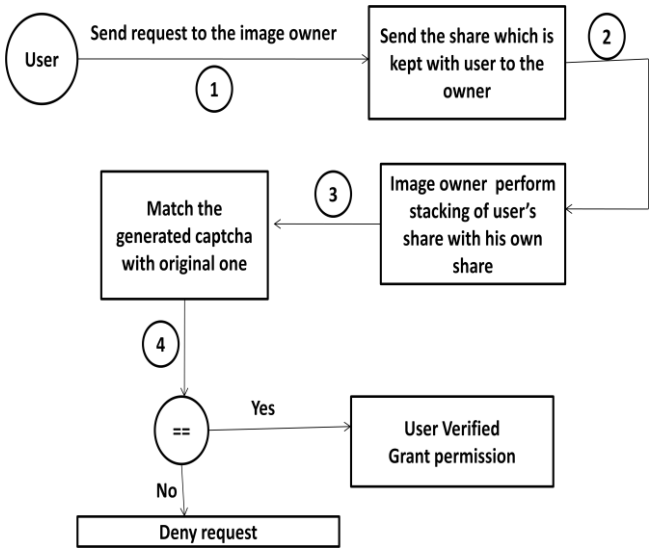

Figure 5(b): Verification

Figure6 (a): Original image captcha and image captcha after shuffling

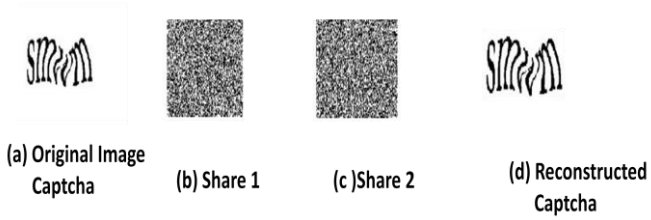

Figure 6(b): sharing and stacking of shares

5.3 Image Decryption

Image decryption is done at the owner/user's machine. After getting encoded results cloud user generates the key for decryption and performs all the operations on the encoded image in reverse.

6. PERFORMANCE ANALYSIS

6.1 Histogram Analysis

Histogram analysis is a kind of attack technique in which images are categorized specifically according to histogram shapes or data. To restrict such attacks, the histogram of the encoded image should be different than that of the original image. We have done experimental analysis of the proposed image encryption algorithm on color image as well as grey image. The plain image Lena with the size 512 × 512 is shown in Fig. 5a and the histogram of the plain image is shown in Fig. 5b. The encrypted image is shown in Fig.5c and the histogram is shown in Fig. 5d. From the figure, we can observe that the histogram of the ciphered image is fairly uniform and is significantly different from that of the original image.

6.2 Correlation Coefficient of adjacent pixels

The correlation between two adjacent pixels in the encoded image is low meaning that the two adjacent pixels in the encoded image are less correlated whereas the correlation between two adjacent pixels in the plain image are high which shows that the two adjacent pixels are highly correlated. To test the correlation of adjacent pixels some simulations are carried out. First of all randomly select 3000 pairs of two adjacent pixels from the image, and then calculate the correlation coefficient of each pair by using the following formulas:

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \quad (11)$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x_i)\right)^2 \quad (12)$$

$$cov(x, y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x_i)\right)\left(y_i - E(y_i)\right) \quad (13)$$

$$rxy = \frac{cov(x,y)}{\sqrt{D(x)D(y)}} \quad (14)$$

Where x and y are gray values of two adjacent pixels in the image. Table 1 shows the simulation result of the proposed algorithm for the image Lena (gray level). The results show that the correlation coefficient is very close to zero in the encrypted image, and thus the proposed algorithm is less predictable and more secure.

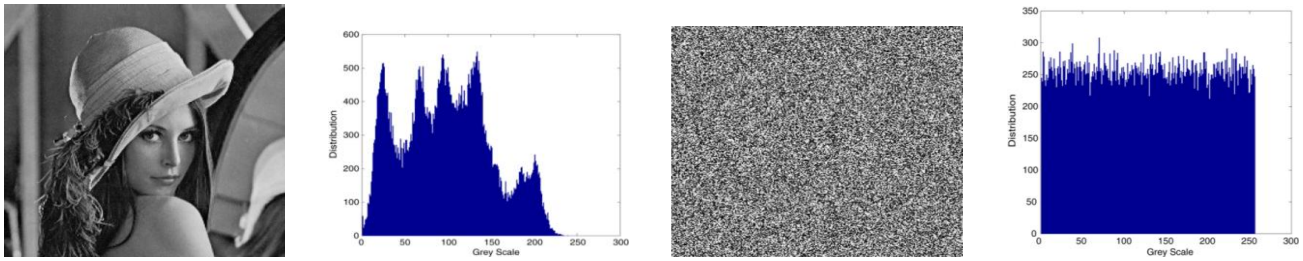

Figure 5: Image Lena (a) Original Image (b) histogram of original Image (c) Encrypted Image (d) histogram of encrypted Image

Table 1: Coefficient of Correlation of plain image and ciphered image

Scan Direction	Image Lena		Image pepper					
	Original Image	Encrypted Image	Original Image			Encrypted Image		
			R	G	B	R	G	B
Horizontal	0.9491	-0.0006	0.9604	0.9778	0.9561	0.0069	-0.0019	-0.0015
Vertical	0.9768	-0.0030	0.9674	0.9796	0.9573	0.0024	0.0033	0.0096
Diagonal	0.9304	0.0061	0.9327	0.9608	0.9195	0.0001	0.0067	-0.0024

7. RESULTS AND CONCLUSION

In this paper we have proposed an image encryption algorithm that enhances the privacy and security of images outsourced to the cloud for storage. One of the features of the proposed scheme that distinguishes it with others is that authentication is also there for the user and all the computations take place without cloud server having the opportunity to gather any intelligence about the images. Image captcha based authentication is very secure method for verifying user's identity. The image Captcha is readable by human users alone and not by machine users. So, using image Captcha technique, no machine based user can crack the password and cannot access the system. And as a third layer of security it prevents intruders' attacks on the user's account. This method provides additional security in terms of not letting the intruder log in into the account even when the user knows the username of a particular user. In this scheme chaotic system is used for encrypting the image, as chaotic system is comparatively cryptographically secure. The experimental results show that the algorithm possesses high security and a large key space. Although for some images its performances goes low but it is effective in most of the cases. In the proposed encryption algorithm there are only some XOR operations and table lookup operations for each pixel therefore it is comparatively fast. Our future work is to enhance the performance of the algorithm for all variety of images.

8. REFERENCES

[1] J.Srinivas, K.Venkata Subba Reddy and Dr. A.Moiz Qyser, "Cloud Computing Basics", International Journal of Advanced Research in Computer and Communication EngineeringVol.1, Issue 5, pp 343-347, 2012.

[2] Chunye Gong, Jie Liu, Qiang Zhang, Haitao Chen and Henghu Gong, "The Characteristics of Cloud

Computing", 39th International Conference on Parallel Processing Workshops, IEEE XPlore, 1530- 2016/10, pp 275-279, 2010.

[3] Karen Scarfone, Murugiah Souppaya, Paul Hoffman, "Guide to Security for Full Virtualization Technologies ",http://csrc.nist.gov/publications/nistpubs/800-125/SP800-125- final.pdf , NIST, 2011.

[4] Stratus Technologies, "white paper on Server Virtualization and CloudComputing:Four hidden impacts on uptime and availability",http://www.stratus.com/~/media/Stratus/Files/Library/WhitePapers /ServerVirtualizationandCloudComputing.pdf , 2011.

[5] Eman M.Mohamed, Hatem S.Abdelkader and Sherif El-Etriby,"Data Security Model for Cloud Computing", The Twelfth International Conference on Networks, ISBN: 978-1-61208-245-5, pp 66-74, 2013.

[6] Peter Mell, Tim Grance, "Effectively and Securely Using the Cloud Computing Paradigm", NIST, Information Technology Laboratory, http://www.csrc.nist.gov/groups/SNS/cloud-computing/cloudcomputing- v26.ppt. 2009.

[7] Frank Gens et al., "Cloud Computing 2010 An IDC Update "http://www.cionet.com/Data/files/groups/Cloud%20Computing%2 02010%20-%20An%20IDC%20Update.pdf ,2010.

[8] D. Song, D. Wagner, and A. Perrig, "Practical techniques for searches in encrypted data," in *Proc. IEEE Int. Symp. Res. Security Privacy*, May 2000, pp. 44–55.

[9] A. Swaminathan, Y. Mao, G.-M. Su, H. Gou, A. L.Varna, S. He,M. Wu,and D. W. Oard, "Confidentiality preserving rank-ordered search," in *Proc. ACM Workshop Storage, Security, Survivabil.*, 2007, pp. 7–12.

[10] W. Lu, A. Swaminathan, A. L. Varna, and M. Wu, "Enabling search over encrypted multimedia databases," *Proc. SPIE*, vol. 7254, pp. 1–11, Jan. 2009.

[11] J. Shashank, P. Kowshik, K. Srinathan, and C. Jawahar, "Private content based image retrieval," in *Proc. IEEE Conf. Comput. Vis. PatternRecognit.*, Jun. 2008, pp. 1–8.

[12] E. Goh, H. Shacham, N. Modadugu, and D. Boneh. Sirius, " Securing remote untrusted storage". In Proceedings of Network and Distributed Systems Security (NDSS) Symposium, pages 131–145, 2003.

[13] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu. Plutus, "Scalable secure file sharing on untrusted storage". In Proceedings of the 2nd USENIX Conference on File and Storage Technologies, pages 29–42, 2003.

[14] Z. Lin and H. Wang, "Image encryption based on chaos with PWL memristor in Chua's circuit," in Proc. of the Int. Conf. on Commun.,Circuits and Systems, July 2009, pp. 964-968.

[15] C. Fu and Z. Zhu, "A chaotic image encryption scheme based on circular bit shift method," in Proc. of the 9th Int. Conf. for Young Computer Scientists, (ICYCS 2008), Nov. 2008, pp. 3057-3061.

[16] G.M.B.S.S. Kumar and V. Chandrasekaran, "A novel image encryption scheme using Lorenz attractor," in Proc. of the 4th IEEE Conf. on Industrial Electronics and Applications, (ICIEA 2009), May, 2009, pp. 3662- 3666.

[17] Omid Mirzaei · Mahdi Yaghoobi · Hassan Irani,"A new image encryption method: parallel sub-image encryption with hyper chaos", Springer Science+Business Media B.V. 2011.

[18] Arash Nourian, Muthucumaru Maheswaran "Towards Privacy Enhanced Limited Image Processing in the Clouds", Doctoral Symposium, Dec 3 2012 Montreal Quebec, Canada 978-1-4503-1611-8/2012 ACM.

[19] A. Shamir, .How to Share a Secret,. Communication ACM, vol. 22, 1979, pp. 612-613.

[20] G. R. Blakley, .Safeguarding Cryptographic Keys,. Proceedings of AFIPS Conference, vol. 48, 1970, pp. 313-317.

[21] A. Menezes, P. Van Oorschot and S. Vanstone, .Handbook of Applied Cryptography,. CRC Press, Boca Raton, FL, 1997.

[22] Von Ahn, Luis; Blum, Manuel; Hopper, Nicholas J.; Langford, John (May 2003). CAPTCHA: Using Hard AI Problems for Security. EUROCRYPT 2003: International Conference on the Theory and Applications of Cryptographic Techniques.

[23] CAPTCHA:Using Hard AI Problems For Security Luis von Ahn1, Manuel Blum1, Nicholas J. Hopper1, and John Langford.