International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-2, December, 2019

Visual Cryptography Based Authentication Technique for Cloud Environment using SVD Factorization

Anupama Jain, R. K. Pateriya

Abstract— World is going toward digitalization and cloud computing plays an important role to connect digital devices for communication with each other. Communication with authentic device and secure its illegal access is the main feature of cloud providers. With the growth of cloud technologies attackers are also finding different attack vectors to break down the cloud authentication system. Previous research illustrates that there is need to develop strong authentication technique to strengthen the trust on cloud systems. This paper demonstrated a visual cryptographic authentication technique for cloud environment. The technique is based on the SVD factorization method. SVD works effectively to create multiple shares of an image and make strong authentication algorithm on the basis of random image feature selection. Result analysis shows that SVD factorization works effectively rather than LU factorization in cloud environment.

Keywords: Cloud Authentication Technique, SVD Factorization, Visual Cryptography, Image factorization, Cloud Security, Tenant Privacy Preservation.

I.INTRODUCTION

The aim of digitalizing the world is user centric by promoting the interconnected digital devices to automate the end user's facilities. This is possible only due to the internet and related advanced technologies like cloud computing. In today's world trust of end user toward cloud computing facilities is accelerating with atomic speed. End users are saving images, videos, and documents online to access anywhere in the world. They are sharing their day to day life, raising voice, finding solutions on finger tips through social media accounts. Marsh and Microsoft [1] surveyed that total number of devices internally connected with internet till 2025 is probably to be 75 billion. In same direction, service providers are also doubling the speed of cloud uses through facilitating easy and fast services like handy payment system, Wi-Fi parks, game zone, and automatically interconnected devices working similar with human mind. All these facilities need digital mechanism to know and serve right contents to right end user. This aim may fulfil through authentication techniques. It prevents illegal access and strengthens the privacy of end user and its contents. Research community proposes various authentication mechanism and protocols for cloud environment such as password based user authentication [2], Research community proposes various authentication mechanism and protocols for cloud environment such as password based user authentication [2], Challenge-response authentication protocols [3], Biometric-based authentication [4], Token-based authentication [5-6], Multi Factor Authentication (MFA) [7], Single sign-on authentication [8], etc. The progress and challenges of these existing techniques have been discussed in our research article [9]. Thereafter, concluded that these all authentication techniques are limited at some points.

Attacker may penetrate these authentication techniques through executing the attacks like Man in the Middle (MITM) Attack [10-11]. The attack vectors may be different to exploit MITM and lure novice end users. One of the attack vectors is to capture the packets in middle and identify the password. Next, may be to delay the network and send the duplicate packet containing encrypted password.

The research gap has been identified in this paper is that the existing authentication techniques for cloud environment requires more efforts. Also, in previous research paper [9] a LU factorization based visual cryptography technique for authenticating the tenants has been explained which is enhanced here by SVD factorization.

The paper presents SVD factorization based visual cryptography technique for cloud authentication purpose. It is contributed in following four key directions-

- In this system password is not stored anywhere in physical form. It prevents from stealing type of attack vectors such as MITM.
- Password is encrypted by algorithm in which random number is used to generate cipher, so cipher will not be same for anytime.
- At registration time it shows preview of images which are not actual images. In which one part of selected image is send to the client in encrypted form. So, original image did not pass over during authentication. It minimizes the chances of MITM attack.
- Image is spliced based on random pixel so next time if same image is spliced, it generate different part to compare with previous spliced part.

The research paper is structured as follows. The recent literature survey with key contribution related to authentication techniques has been presented in Section II. Section III illustrates the outline of the working of SVD factorization for visual cryptography based authentication technique.

Revised Manuscript Received on December 30, 2019.
* Correspondence Author
Anupama Jain*, pursuing Ph.D., Department of CSE, MANIT Bhopal (M. P.) India. E-mail: anupamajain575@gmail.com
R. K. Pateriya*, Associate Professor, Department of CSE, MANIT Bhopal (M. P.) India. E-mail: pateriyark@gmail.com

Result has been discussed with mathematical proof and graphs in section IV. Finally, the section V concluded the work with future perspectives of work enhancement.

II.LITERATURE REVIEW

In this section literature review of the visual cryptography techniques and SVD techniques have been carried out. It enhances the proposed technique to focus on to resolve the identified research gaps.

Table 1: Key Contributions of research work

Sr. No.	Title Work	Research Method	Key Contribution
1	Cloud authentication based on encryption of digital image using edge detection [12]	This paper presented two-factor authentication method for cloud computing to reduce the weakness of existing authentication methods. As first factor it popup OTP to tenant and uses partial encryption of an image as second factor. The encryption method is based on edge detection technique.	Author claims that presented method is capable to prevent form attacks and issues such as stolen-verifier issue, MITM Seed tracing, on-line or off-line presumption attack, insider attack, dictionary attack, reflection attack, replay attack, etc.
2	Asynchronous Challenge-Response Authentication Solution based on Smart Card in Cloud Environment [13]	This paper presented an asynchronous challenge response authentication method. It utilizes the hash function, random number and combined secret key to generate authentication token once during communication. It also utilizes encryption cards and encryption machine to encrypt and decrypt the credentials of cloud tenant in hardware.	Produce the authentication token once makes it strong and secure in addition with hash value and combined secret key. Token have the session value and expire in time which prevents from the replay attack. Random number generation by cryptography method prevents from guessing attack.
3	Image based Authentication with Secure Key Exchange Mechanism in Cloud [14]	This paper presented an authentication technique based on Image. At first, tenant authenticates itself through image based authentication technique. Thereafter, tenant creates a key and calculates a unique identification number on the basis of key. Finally, pass that generated number in place of key to CSP. CSP calculate the key reverse form share number at the server side.	Sharing the number in place of credentials protect form replay attack, Impersonation attack, MitM attack, insider attack, etc. It depends on the secrecy of method of number calculation.
4	A Client-Based User Authentication and Encryption Algorithm for Secure Accessing to Cloud Servers based on modified Diffie-Hellman and RSA small-e [15]	This paper mainly focuses on two concepts one to preserve privacy of end user contents and second to secure sharing of credentials. For privacy preservation it demonstrated encryption based on client-based encryption method. Secure sharing of credentials modified Diffie-Hellman and RSA small-e has been used.	Client based encryption model minimizes the chance of content hacking and unauthorized access it. Diffie-Hellman and RSA small-e make sharing secure and penetration free.
5	A strong user authentication framework for cloud computing [16]	This paper demonstrated two-step verification through smart card and password. Also demonstrated the mutual authentication, identity management and session key setup. It is more effective to preserve end user privacy.	It can prevent from the attacks such as replay attack, MITM DoS, etc.
6	Encrypting Informative Colour Image using Colour Visual Cryptography [17]	This paper presented two-out-of-two secret sharing visual cryptography method to encrypt colour images. This method breaks input colour image into two parts in a way that only one part is not enough to predict its small portion of original image. Original image can be regained by X-OR operation of both parts.	Proposed method does not require complex mathematical calculations. So, the image size of regained image does not increase more and negligible amount of noise is introduced. But, user can see structure of image by overlapping the both parts.

7	Towards the Growth of Image Encryption and Authentication Schemes [18]	This survey paper focused on types of authentication methods and visual encryption methods for versions of images with their pros and cons.	Finally concluded that both the visual cryptography and the authentication techniques need enhancement for secure technology development.
8	Signature Based Authentication using Contrast Enhanced Hierarchical Visual Cryptography [19]	This paper presented authentication method based on hierarchical visual cryptography. It encrypts the end users' digital-signature by generating its four parts. In which any three parts are used to generate key part. It stored at server side after registering the user. During authentication end user sends remaining share to server for authentication. Superimposing of image's key part and remaining parts generate original image for verification of credentials.	The Hierarchical visual cryptography method hierarchically encrypts the input image which enhances the confidentiality of credentials in different parts of image.

III. VISUAL CRYPTOGRAPHY USING SVD FACTORIZATION

Visual Cryptography technique used to encrypt the visual information like image, text into multiple shares of visual images. SVD factorization is generalization of Eigen decomposition of positive semi definite normal matrix to m × n matrix via an extension of polar decomposition. This factorization can be applied on a real and complex matrix and has application in signal processing and statics. In SVD factorization, matrix A is decomposed in following way:

$$A = U\Sigma V^{T}$$

Where-
A = m × n matrix which is to be decomposed
U = m × m unitary matrix, whose columns are the left singular vectors,
Σ = m × n rectangular diagonal matrix has singular values,
V = n × n unitary matrix whose columns are right singular vectors.

Because of properties of SVD factorization method described above, classification of matrix factorization will be used in our proposed work. Since in proposed work, is used to split the image so the description and advantage has been given in detailed as below:

To find out the value of U and V, the Eigen value and Eigen vector of AA^T and A^TA is calculated. Let matrix A is

$$A = \begin{bmatrix} a & b & \cdot & \cdot & \cdot \\ c & d & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}_{m\times n}$$

The matrix U is determined in following way:

$$AA^T = \begin{bmatrix} a & b & \cdot & \cdot & \cdot \\ c & d & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}_{m\times n} \begin{bmatrix} a & c & \cdot & \cdot \\ b & d & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}_{n\times m}$$

$$= \begin{bmatrix} p & q & \cdot & \cdot \\ r & s & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}_{m\times m}$$

Eigen value and Eigen vector is calculated by using following expression:

$$\det(AA^T - \lambda I) = 0$$

The above equation gives real Eigen value of $\lambda_1, \lambda_2, \lambda_3, \ldots\ldots \lambda_m \geq 0$. Now, Eigen vector will be calculated for each $\lambda_1, \lambda_2, \lambda_3, \ldots\ldots \lambda_m$ in following way:

$$(AA^T - \lambda_k I)v_k = 0,$$

where, $k = 1, 2, 3, \ldots\ldots m$

For λ_1, v_1 will be-

$$v_1 = \begin{pmatrix} v_{11} \\ v_{12} \\ \cdot \\ \cdot \\ v_{1m} \end{pmatrix}$$

Similarly for λ_2, v_2 will be-

$$v_2 = \begin{pmatrix} v_{21} \\ v_{22} \\ \cdot \\ \cdot \\ v_{2m} \end{pmatrix}$$

For λ_m, v_{1m} will be-

$$v_m = \begin{pmatrix} v_{m1} \\ v_{m2} \\ \cdot \\ \cdot \\ v_{mm} \end{pmatrix}$$

Since in SVD, columns of U are left singular vector therefore,

$$U = [v_1 \quad v_2 \quad \cdot \quad \cdot \quad v_m]_{m\times m}$$

Similar way will be followed to calculate the matrix V. The steps are-

$$A^TA = \begin{bmatrix} a & c & \cdot & \cdot \\ b & d & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}_{n\times m} \begin{bmatrix} a & b & \cdot & \cdot & \cdot \\ c & d & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot & \cdot \end{bmatrix}_{m\times n}$$

$$= \begin{bmatrix} e & f & \cdot & \cdot \\ g & h & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot & \cdot \end{bmatrix}_{n\times n}$$

Eigen value and Eigen vector is calculated by using following expression:

$$\det(A^TA - \lambda I) = 0$$

The above equation gives real Eigen value of $\lambda_1, \lambda_2, \lambda_3, \ldots\ldots \lambda_n \geq 0$. Now, we will calculate the Eigen vector for each $\lambda_1, \lambda_2, \lambda_3, \ldots\ldots \lambda_n$ in following way:

$$(AA^T - \lambda_j I)v_j = 0,$$

where, $j = 1, 2, 3, \ldots\ldots n$

For λ_1, v_1 will be-

$$v_1 = \begin{pmatrix} v_{11} \\ v_{12} \\ \cdot \\ \cdot \\ v_{1n} \end{pmatrix}$$

Similarly, for λ_2, v_2 will be-

$$v_2 = \begin{pmatrix} v_{21} \\ v_{22} \\ \cdot \\ \cdot \\ v_{2n} \end{pmatrix}$$

For λ_n, v_{1n} will be-

$$v_n = \begin{pmatrix} v_{n1} \\ v_{n2} \\ \cdot \\ \cdot \\ v_{nn} \end{pmatrix}$$

Since in SVD, columns of V are right singular vector therefore,

$$V = [v_1 \quad v_2 \quad \cdot \quad \cdot \quad v_n]_{n\times n}$$

$$V^T = \begin{bmatrix} v_1 \\ v_2 \\ \cdot \\ \cdot \\ v_n \end{bmatrix}_{n\times n}$$

Σ is $m \times n$ rectangular diagonal matrix has singular value $(\sigma_1, \sigma_2, \sigma_3, \ldots \sigma_m)$ which is calculated by taking square root of Eigen value of AA^T

$$\Sigma = dia(\sigma_1, \sigma_2, \sigma_3, \ldots \sigma_m)$$

$$\Sigma = \begin{bmatrix} \sigma_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \sigma_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \cdot & 0 & 0 & 0 \\ 0 & 0 & 0 & . & 0 & 0 \\ 0 & 0 & 0 & 0 & \sigma_m & 0 \end{bmatrix}_{m\times n}$$

After calculating the U, Σ, V the matrix A can be represented in following decomposition form:

$$A = U\Sigma V^T$$

$$A = [v_1 \quad v_2 \quad \cdot \quad \cdot \quad v_m]_{m\times m} \begin{bmatrix} \sigma_1 & 0 & 0 & 0 & 0 & 0 \\ 0 & \sigma_2 & 0 & 0 & 0 & 0 \\ 0 & 0 & \cdot & 0 & 0 & 0 \\ 0 & 0 & 0 & . & 0 & 0 \\ 0 & 0 & 0 & 0 & \sigma_m & 0 \end{bmatrix}_{m\times n} \begin{bmatrix} v_1 \\ v_2 \\ \cdot \\ \cdot \\ v_n \end{bmatrix}_{n\times n}$$

IV.RESULT ANALYSIS

The result analysis of the proposed work has been carried out and presented here in two ways. Firstly, proposed authentication process has been proved mathematically through proving the SVD for n*n images. Secondly, verify the correctness of proposed authentication mechanism using the widely-accepted performance parameters based on confusion matrix.

In proposed work the shares of image is created using matrix factorization. Hence, first it has been proved the SVD is suitable for proposed work for image of n*n pixels. In matrix factorization, the matrix is factorized into product of matrices.

A. Mathematiical corroboration

The SVD factorization can be applied on pixel value of an image. The image can be split by factorizing the matrix of pixel value of an image. Here, the SVD factorization of given image is described below:

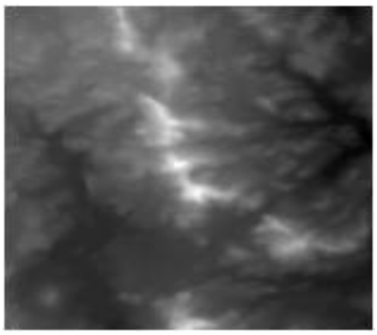

Fig.1: Sample Image to Mathematically Evaluate SVD factorization for Visual Cryptography based Authentication Technique

For given image, the matrix of pixel value is given below:

$$A = \begin{bmatrix} 252 & 249 & 246 & 243 & 237 \\ 255 & 255 & 250 & 246 & 243 \\ 253 & 254 & 248 & 245 & 243 \\ 250 & 249 & 245 & 243 & 239 \end{bmatrix}$$

Find out U matrix:

$$AA^T = \begin{bmatrix} 301239 & 306624 & 305136 & 300963 \\ 306624 & 312115 & 310604 & 306350 \\ 305136 & 310604 & 309103 & 304868 \\ 300963 & 306350 & 304868 & 300696 \end{bmatrix}$$

$$\det(AA^T - \lambda I) = \begin{bmatrix} 301239-\lambda & 306624 & 305136 & 300963 \\ 306624 & 312115-\lambda & 310604 & 306350 \\ 305136 & 310604 & 309103-\lambda & 304868 \\ 300963 & 306350 & 304868 & 300696-\lambda \end{bmatrix}$$

On solving this equation, obtain the eigen values that is λ_1=1.22314×106, λ_2=10.075, λ_3=2.32125, λ_4= 0.0744932. Now, calculate Eigen vector by using following expression:

$$\begin{bmatrix} 301239-\lambda & 306624 & 305136 & 300963 \\ 306624 & 312115-\lambda & 310604 & 306350 \\ 305136 & 310604 & 309103-\lambda & 304868 \\ 300963 & 306350 & 304868 & 300696-\lambda \end{bmatrix} v = 0$$

For λ_1=1.22314×106, Eigen vector v_1 will be-

$$v_1 = \begin{pmatrix} 1.00079 \\ 1.01883 \\ 1.01391 \\ 1 \end{pmatrix}$$

Similarly, for λ_2=10.075, Eigen vector v_2 will be-

$$v_2 = \begin{pmatrix} -29.3171 \\ 5.75677 \\ 22.1705 \\ 1 \end{pmatrix}$$

Similarly, for λ_3=2.32125, Eigen vector v_3 will be-

$$v_3 = \begin{pmatrix} -0.172949 \\ -0.727012 \\ -0.0850278 \\ 1 \end{pmatrix}$$

Similarly, for λ_4= 0.0744932, Eigen vector v_4 will be-

$$v_4 = \begin{pmatrix} -0.99728 \\ 1.82775 \\ -1.83844 \\ 1 \end{pmatrix}$$

$$A^TA = \begin{bmatrix} 255038 & 254285 & 249736 & 246701 & 242918 \\ 254285 & 253543 & 249001 & 245974 & 242211 \\ 249736 & 249001 & 244545 & 241573 & 237871 \\ 246701 & 245974 & 241573 & 238639 & 234981 \\ 242918 & 242211 & 237871 & 234981 & 231388 \end{bmatrix}$$

On solving this equation, we get the Eigen values that is λ_1=1.5166×106, λ_2=-348524, λ_3=16.3974, λ_4= 1.2119, λ_5 = 0.107466. Hence, for λ_1=1.5166×106, Eigen vector v_1 will be-

$$v_1 = \begin{pmatrix} 2.48468 \\ 1.04672 \\ 1.02808 \\ 1.01556 \\ 1 \end{pmatrix}$$

Similarly, for λ_2=-348524, Eigen vector v_2 will be

$$v_2 = \begin{pmatrix} -5.42028 \\ 1.04682 \\ 1.02814 \\ 1.01564 \\ 1 \end{pmatrix}$$

Similarly, for λ_3=16.3974, Eigen vector v_3 will be-

$$V = \begin{bmatrix} 2.48468 & -5.42028 & -1.63431 \\ 1.04672 & 1.04682 & 0.693601 \\ 1.02808 & 1.02814 & -0.00993679 \\ 1.01556 & 1.01564 & -9.853217507703 \ldots \times 10^{-6} \\ 1 & 1 & 1 \end{bmatrix}$$

Since for SVD factorization, we need V^T

$$V^T = \begin{bmatrix} 2.48468 & 1.04672 & 1.02808 & 1.01556 & 1 \\ -5.42028 & 1.04682 & 1.02814 & 1.01564 & 1 \\ -1.63431 & 0.693601 & -0.00993679 & -9.853217507703 \ldots \times 10^{-6} & 1 \\ 0.991823 & -0.678633 & -1.29459 & 1.465129708942..\times 10^{-6} & 1 \\ 5.15282 & 0.709938 & -6.95779 & 2.713127043029 \ldots \times 10^{-7} & 1 \end{bmatrix}$$

In SVD, Σ is singular value diagonal matrix and singular value of matrix is calculated by taking square root of Eigen value of matrix for following assuming matrix the Eigen values are 11, 1, 0 and the singular values are-

$$\sigma_1 = \sqrt{1.22314 \times 106}, \quad \sigma_2 = \sqrt{10.075}, \quad \sigma_3 = \sqrt{2.32125}, \quad \sigma_4 = \sqrt{0.0744932}$$

Therefore, Σ will be-

$$\Sigma = \begin{bmatrix} \sqrt{1.22314 \times 106} & 0 & 0 & 0 & 0 \\ 0 & \sqrt{10.075} & 0 & 0 & 0 \\ 0 & 0 & \sqrt{2.32125} & 0 & 0 \\ 0 & 0 & 0 & \sqrt{0.0744932} & 0 \end{bmatrix}$$

We have found the U, Σ, V^T therefore, the SVD factorization assumed matrix A will be-

Since columns of U are left singular vector therefore,

$$U = \begin{bmatrix} 1.00079 & -29.3171 & -0.172949 & -0.99728 \\ 1.01883 & 5.75677 & -0.727012 & 1.82775 \\ 1.01391 & 22.1705 & -0.0850278 & -1.83844 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

Similarly, we will find out V by calculating Eigen value and Eigen vector of A^TA such that-

$$\det(A^TA - \lambda I) = \begin{bmatrix} 255038-\lambda & 254285 & 249736 & 246701 & 242918 \\ 254285 & 253543-\lambda & 249001 & 245974 & 242211 \\ 249736 & 249001 & 244545-\lambda & 241573 & 237871 \\ 246701 & 245974 & 241573 & 238639-\lambda & 234981 \\ 242918 & 242211 & 237871 & 234981 & 231388-\lambda \end{bmatrix}$$

$$v_3 = \begin{pmatrix} -1.63431 \\ 0.693601 \\ -0.00993679 \\ -9.853217507703 \ldots \times 10^{-6} \\ 1 \end{pmatrix}$$

Similarly, for λ_4= 1.2119, Eigen vector v_4 will be-

$$v_4 = \begin{pmatrix} 0.991823 \\ -0.678633 \\ -1.29459 \\ 1.465129708942..\times 10^{-6} \\ 1 \end{pmatrix}$$

Similarly, for λ5= 0.107466, Eigen vector v_5 will be-

$$v_5 = \begin{pmatrix} 5.15282 \\ 0.709938 \\ -6.95779 \\ 2.713127043029 \ldots \times 10^{-7} \\ 1 \end{pmatrix}$$

Since columns of V are right singular vector therefore,

$$V = \begin{bmatrix} 2.48468 & -5.42028 & -1.63431 & 0.991823 & 5.15282 \\ 1.04672 & 1.04682 & 0.693601 & -0.678633 & 0.709938 \\ 1.02808 & 1.02814 & -0.00993679 & -1.29459 & -6.95779 \\ 1.01556 & 1.01564 & -9.853217507703 \ldots \times 10^{-6} & 1.465129708942..\times 10^{-6} & 2.713127043029 \ldots \times 10^{-7} \\ 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

$$A = \begin{bmatrix} 1.00079 & -29.3171 & -0.172949 & -0.99728 \\ 1.01883 & 5.75677 & -0.727012 & 1.82775 \\ 1.01391 & 22.1705 & -0.0850278 & -1.83844 \\ 1 & 1 & 1 & 1 \end{bmatrix}$$

$$\begin{bmatrix} \sqrt{1.22314 \times 106} & 0 & 0 & 0 & 0 \\ 0 & \sqrt{10.075} & 0 & 0 & 0 \\ 0 & 0 & \sqrt{2.32125} & 0 & 0 \\ 0 & 0 & 0 & \sqrt{0.0744932} & 0 \end{bmatrix}$$

$$\begin{bmatrix} 2.48468 & 1.04672 & 1.02808 & 1.01556 & 1 \\ -5.42028 & 1.04682 & 1.02814 & 1.01564 & 1 \\ -1.63431 & 0.693601 & -0.00993679 & -9.853217507703 \ldots \times 10^{-6} & 1 \\ 0.991823 & -0.678633 & -1.29459 & 1.465129708942. . \times 10^{-6} & 1 \\ 5.15282 & 0.709938 & -6.95779 & 2.713127043029 \ldots \times 10^{-7} & 1 \end{bmatrix}$$

The calculated matrix factorization represents the one share of a given image in Figure 1. As per the calculated matrix factorization two image shares are shown in Figure 2.

Fig. 2. Two Image Shares Created by the SVD Factorization based on Visual Cryptography Technique for Authentication

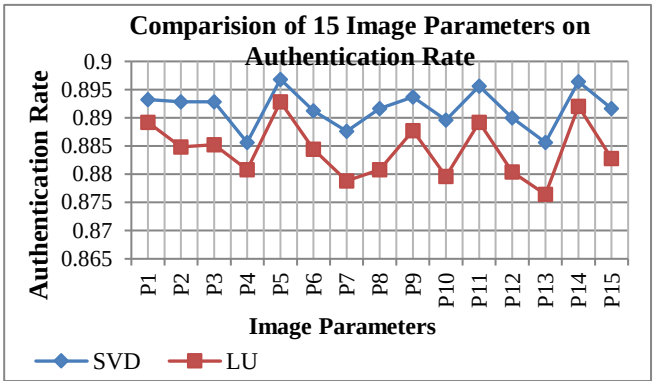

Fig. 3. Comparison of Authentication Rate obtained for proposed system through SVD and LU Factorization at 15 parameters.

B. Result Discussion thorugh Efficiency Parameters

Result discussion of the proposed authentication mechanism is carried out to evaluate the robustness of the authentication mechanism using LU and SVD factorization differently. It has been evaluated through implementing the idea in cloudsim using the JavaScript and PHP.

For analyzing the system standard image dataset has been downloaded and result analysis has been carried out at 15 different parameters represented in this work as P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{12}, P_{13}, P_{14} & P_{15}. Details of parameters are mentioned in previous research paper [9]. Standard Image Data Sets used here are CASIA v1.0, CASIA v2.0, Columbia and IFS-TC.

Efficiency parameters like Authentication Rate, accuracy and F1-score are calculated to compare the LU factorization and SVD Factorization based visual cryptography technique for authenticating cloud tenants at all fifteen parameters. Comparison of authentication rate between both techniques is shown in Figure 3.

Average authentication rate for SVD based visual cryptography for authenticating cloud tenants is 89.16333%. Rather for LU factorization authentication rate is calculated 88.43477%. It shows that SVD factorization for visual cryptography based authentication of cloud technique work more positively rather than LU factorization.

It represents that it works good enough for true positive cases and the chance of authenticating the right user rightly is more in comparison with LU factorization. Further, accuracy has been calculated for both techniques at all fifteen parameters as shown in Figure 4.

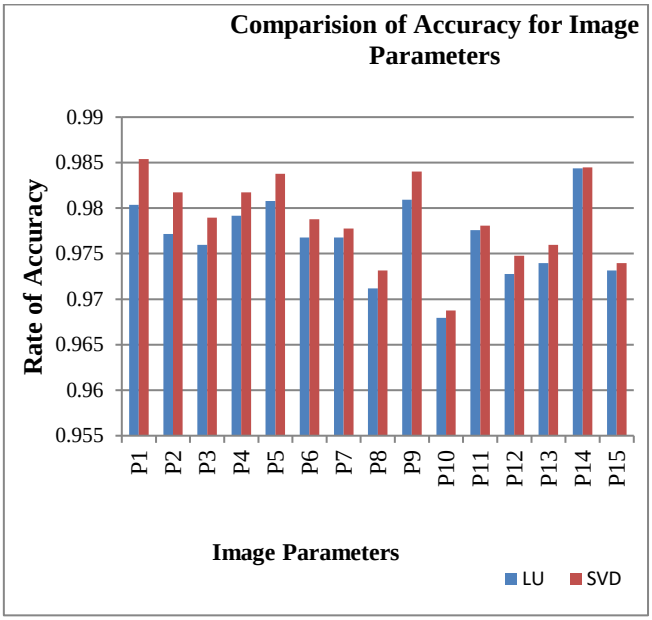

Fig. 4. Comparison of Accuracy obtained for proposed system through SVD and LU Factorization at 15 parameters.

Average accuracy of SVD factorization for fifteen parameters is 97.87580% and for LU factorization is 97.65954%. It shows that SVD factorization for visual cryptography based authentication of cloud technique gives more accurate result in comparison with LU factorization.

Sometimes model having more accuracy cannot be considered effective due to the imbalance between precession and recall. Hence, comparison of both techniques at all fifteen parameters has been strongly carried out through calculating the F1-Score as shown in Figure 5.

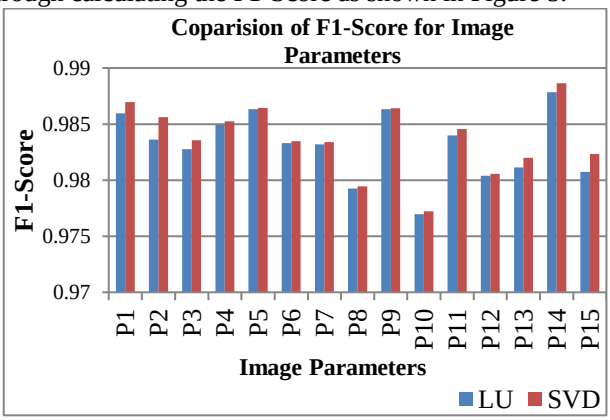

Fig. 5. Comparison of F1-Score obtained for proposed system through SVD and LU Factorization for 15 parameters.

In figure 5, the F1-score of the proposed authentication mechanism for both LU and SVD factorization for all fifteen parameters representing the balance between the precision and the recall. Here, average F1-score of LU is 0.98311 and for SVD is 0.98373 which is more towards the 1 rather LU factorization. It shows that SVD is more stable rather LU factorization.

V.CONCLUSION AND FUTURE WORK

The utility of proposed authentication mechanism is its random security mechanism that makes it enough secure authentication technique. Cloud tenants has to register with this system; in which all information is encrypted that is send to server and vice versa. During registration once end user has to select only one image out of random images. These images are just preview of actual images those cannot be captured and stored at the server end. Again randomization has been applied to get split the image in shares. One share of that image has been encrypted at client end to prevent from the MITM type of attack vectors discussed in this paper.

In this paper SVD factorization based cryptography technique has been represented in comparison of LU factorization. The results of SVD are authentication rate 89.16333%, accuracy 97.87580% and F1-score 0.98373. It shows that SVD works more effectively in comparison with LU factorization. In future the proposed authentication method can be analyzed for different factorization methods and image parameters to get best result.

REFERENCES

1. Marsh & Microsoft, “2019 Global Cyber Risk Perception Survey” [online], september 2019, Available: https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf.
2. M. Babaeizadeh, M. Bakhtiari and A. M. Mohammed, “Authentication Methods in Cloud Computing: A Survey”, Research Journal of Applied Sciences, Engineering and Technology 9(8): 655-664, 2015.
3. G. Zhao, et Al., “Asynchronous challenge-response authentication solution based on smart card in cloud environment”, IEEE, 2nd International Conference on Information Science and Control Engineering, 2015, pp 156-159.
4. S. Sharma and V. Balasubramanian “A biometric based authentication and encryption framework for sensor health data in cloud”, IEEE, International Conference on Information Technology and Multimedia (ICIMU), Putrajaya, Malaysia, 2014, pp. 49-54.
5. O. Ethelbert, F. F. Moghaddam, P. Wieder and R. Yahyapour, "A JSON Token-Based Authentication and Access Management Schema for Cloud SaaS Applications," 2017 IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), Prague, 2017, pp. 47-53.
6. B. Eddine Sabir, Md. Youssfi, O. Bouattane, & H. Allalia, “Authentication and load balancing scheme based on JSON Token For Multi-Agent Systems”, Elsevier, Procedia Computer Science, Vol. 148, 2019, pp. 562-570.
7. A. J. Choudhury, et Al. “A strong user authentication framework for cloud computing” IEEE Computer Society, Int. conf. on Asia- Pacific Services Computing, 2011, pp. 110-115.
8. U. Seddigh, “Evaluation of Single Sign-On Frameworks, as a Flexible Authorization Solution- OAuth 2.0 Authorization Framework”, [Online]. Department of Computer Science, Linnaeus University, Sweden, Available: http://www.diva-portal.se/smash/get/diva2:750217/FULLTEXT01.pdf
9. A. Jain & R. K. Pateriya, “An Authentication Method based on Visual Cryptography for Cloud Environment”, International Journal of Engineering and Advanced Technology (IJEAT), Vol:8, Issue:6, 2019.
10. Symantec employee, “What is a man-in-the-middle attack?” [Online], Norton, Available: https://us.norton.com/internetsecurity-wifi-what-is-a-man-in-the-middle-attack.html
11. S. Anand & V. Perumal, “EECDH to prevent MITM attack in cloud computing”, KeAi, In Press: Digital Communications Networks, 2019.
12. Ali A. Yassin, Abdullah A. Hussain, Keyan Abdul-Aziz Mutlaq, “Cloud authentication based on encryption of digital image using edge detection”, IEEE, the Int. Symposium on Artificial Intelligence and Signal Processing (AISP), 2015, Iran.

13. Guifen Zhao, Ying Li, Liping Du & Xin Zhao, "Asynchronous Challenge-Response Authentication Solution Based on Smart Card in Cloud Environment", IEEE, 2nd Int. Conf. on Information Science and Control Engineering (ICISCE-15), 2015, Shanghai, China.
14. A. S. Tomar, G. Ku. Tak, & R. Chaudhary, "Image based authentication with secure key exchange mechanism in cloud", IEEE, Int. Conf. on Medical Imaging, m-Health and Emerging Communication Systems (MedCom), 2014, Greater Noida, India.
15. F. Fatemi Moghaddam, S. D. Varnosfaderani, Iman Ghavam & S. Mobedi, "A client-based user authentication and encryption algorithm for secure accessing to cloud servers based on modified Diffie-Hellman and RSA small-e", IEEE Student Conference on Research and Development, 2013, Putrajaya, Malaysia.
16. A. Jyoti Choudhury, P. Kumar, M. Sain & H. Lim, & Hoon Jae-Lee, "A Strong User Authentication Framework for Cloud Computing", EEE Asia-Pacific Services Computing Conference, 2011, Jeju Island, South Korea.
17. P. V. Chavan & R.S. Mangrulkar, "Encrypting Informative Color Image Using Color Visual Cryptography", IEEE, 3rd International Conference on Emerging Trends in Engineering and Technology, 2010, Goa, India
18. A. S. Rajput, N. Mishra & S. Sharma, "Towards the growth of image encryption and authentication schemes", IEEE, International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2013, Mysore, India.
19. P. V. Chavan, Md. Atique & L. Malik, "Signature based authentication using contrast enhanced hierarchical visual cryptography", IEEE Students' Conference on Electrical, Electronics and Computer Science, 2014, India

AUTHORS PROFILE

Anupama Jain, is currently pursuing her PhD from Maulana Azad National Institute of Technology, Bhopal. She received her Master's degree from Department of CSE, UIT BU, Bhopal, India in 2008. With sixteen years of teaching experience in SATI Vidisha and SIRT Bhopal colleges, she has good knowledge in various computer science subjects. Her current research interest includes information security, distributed system and cloud computing.

R. K. Pateriya, is an Associate Professor in the CSE Department at Maulana Azad National Institute of Technology, Bhopal. He received his PhD in 2011 and has more than 26 year of teaching experience in MANIT, an Institute of National Importance. He has guided many UG, PG and Ph.D students, his research work has been published in various reputed journalsand conferences which includes SCI, IEEE, Scopus and Web of Science Index. His current research interest includes information security, cloud computing, e-commerce, data mining and information retrieval.