Enhancing the Security of Cloud Computing: Genetic Algorithm and Qr Code Approach

Dr. Vanaparthy Ramarao

Associate Professor, Gandhi Academy of Technical Education, Kodad.

ABSTRACT:

Paradigms of Cloud computing square measure gaining prevalent acceptance thanks to the various edges they provide. These comprise cost-effectiveness, time savings and effective readying of computing resources. However, privacy and security problems square measure among the main hindrances holding back the widespread adoption of this novel technology. In this context, enhancing the protection of cloud computing demands the very best priority supported the popular encoding method RSA, Genetic formula (GA), and 3D fast Response (QR) code victimisation mack address. This paper can show an approach of amplifying the protection of cloud computing. Therefore, we tend to square measure proposing advanced ballroom dance security mechanism of cloud computing. Firstly, RSA is employed to produce initial protection of the primary stratum. RSA approaches message as input to the hash perform and generated hash values is encrypted by victimisation generated sender key. and therefore the receiver can generate a hash code and decrypts the message victimisation the sender's public key. Finally, The Genetic algorithms (GA) square measure generalized search algorithms supported the mechanics of natural genetic science. GA maintains a population of people that represent the candidate solutions. when thriving completion of Genesis, mutation and crossover GA can give a framework to match the specified pattern. Moreover, a media access management address (MAC address) of a tool may be a distinctive symbol allotted to network interfaces for communications at the information link layer of a network section. In this context, the mack address is employed to come up with the 3D fast response code for user verification. Through experiments, we affirm that the mixture of GA and 3D QR Code approach with RSA for ballroom dance security mechanism shows robust potential to heighten the protection of Cloud Computing.

Keywords: cloud computing; RSA algorithm; genetic algorithm;Face Recognition; 3D QR code.

1. INTRODUCTION

Cloud computing is a lot of intimate during this innovative epoch. this can be a general that means for wont to compromise a new step of network-based computing that may happen over the LAN. it's an excellent attention from people at home to any or all governments in each of publications and among users. it's clear to state, Cloud computing becomes a lot of popular to store knowledge and victimisation knowledge within the network while not using hardware. currently each day the safety statement could be a huge question of Cloud Computing. There ar the foremost vital data and also the data is losing in daily for the shortage of ensuring security. the safety improvement is that the lone means to succeed in the top. This improvement

will be processed by RSA algorithmic rule, Face Recognition by Genetic algorithmic rule, Generate 3D QR code of a singular waterproof address. RSA cryptosystem was designed in 1977 by Ron Rivest, Adi Shamir, and author Adelman. this method could be a a lot of popular public key algorithmic rule for its simplicity. This security stands to calculate the weather of an enormous composite whole number. Currently factorization 1024 bits whole number is assumed to be as complex because the employment of 280 that is that the current benchmark utilized in cryptography. The high management price and storage usage bring the algorithmic rule within the analysis space [1]. face expression recognition by a pc will be parted into 2 approaches ar constitutionally based mostly and facing-based. In constituent-based access, recognition is founded on the link in human facial characteristics like as eyes, lip, nose, profile silhouettes and face boundary [2]. Genetic algorithmic rule, that is currently each day at the best used and efficient algorithmic rule within the passing generation. It mainly performs 3 steps for checking. Those steps ar Mutation, Crossover, and Genesis. The persistence of mutation in Gas is preserving and introducing diversity. it's a genetic operator, that maintains genetic diversity from one generation of a population of genetic algorithmic rule chromosomes to succeeding. Then the crossover is that the different constituent of the Genetic algorithmic rule that primarily applied for the matching. In our operation, this can be the most ingredient. Genesis is that the closing element of GA which is employed for mutation and crossover formula within the programming section [3]. waterproof

could be a lasting and really distinctive identity of a tool with networking capability that is recognized additionally as a Network Interface Card (NIC). The MAC address could be a 48-bit binary variety that's contained in plaintext frame that is transmitted in network property [4]. The waterproof address is decided to use with the information link layer. It is also referred to as the Physical address of a hardware. A barcode is AN optical machine-readable representation of information, that presents data regarding attaching the article. 3D QR code consists of AN array 3D cells, referred to as modules, it became either stuffed or empty, corresponding to doable values of a chunk. The created 3D construction permits for rather more data-storage capability inside the codification. It contains knowledge not simply in its coordinate axis and coordinate axis however thorough additionally [5].

2. METHODOLOGY

In this half, we are going to discuss however our planned theme will operate in reality. Methodology section consists of several subsections wherever coding technique, registration

process, and knowledge matching techniques are going to be explained in details with their various method diagram and flow chart. Fig.1. indicates the flow chart of RSA formula wherever the running operation of that individual formula shows in particular.

A. Username and countersign coding and cryptography Signing method of users can extend through the RSA algorithm wherever the coding and cryptography can take place. 2 step procedure for user registration is clearly depicted in Fig.1. With a flow chart.

International Journal of Research

Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Step-1: The RSA system can operate each public and private key wherever it'll construct a mix of those and coding of messages will be performed employing an equivalent methodology.

Step-2: Here, the values ar encrypted and decrypted with C=ME mod N

B. Registration method

After winning completion of the initial steps, the following element of registration offers user two kinds of alternative picks like Face Recognition and 3D QR code. clarification and dealing method of every step area unit summarized here. Fig.2. Indicates that however this registration model works for users.

Step-1: In step one initial security layer of the developed system is shown wherever the info is employed to finish the registration method. Users have to be compelled to enter [username,

password] for the login technique. The username are taken to the info with some garbage string and also the Arcanum will be encrypted victimisation RSA cryptosystem.

Step-2: when cryptography, this method sets up 2 choices for users (Option one or possibility 2)

Choice 1: The Genetic rule is applied to acknowledge the facial expressions, whereas during this composition, we will try five sample pictures to place through this technique.

Choice 2: By victimisation the mackintosh address of device possibility 2 will generate a novel information for QR code.

Step-3: Execution of winning information matches with the database, therefore the user can receive the permission to access.
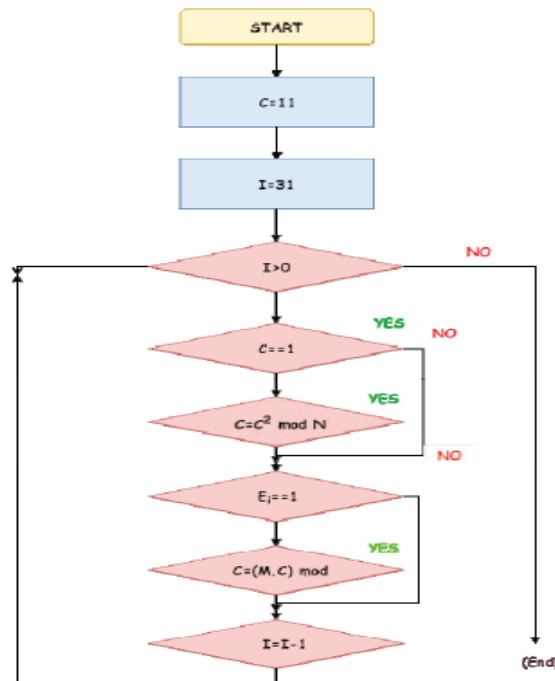

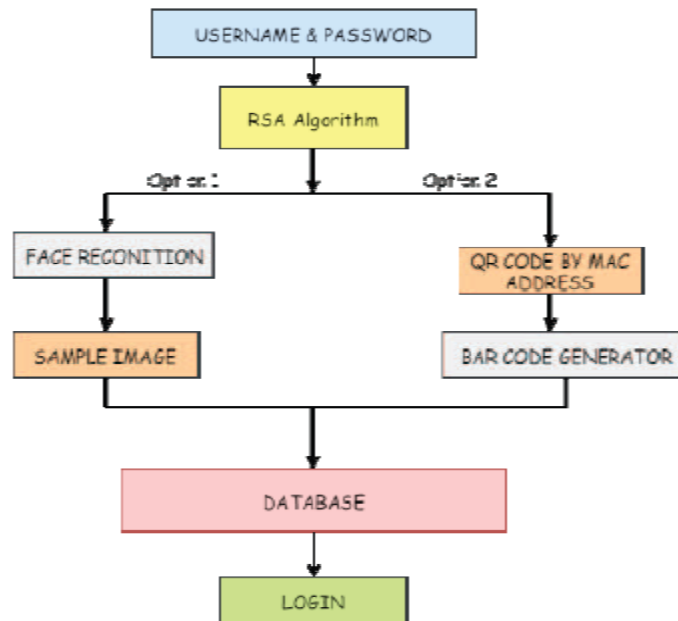Fig.1: Flowchart of RSA Algorithm for encryption and decryption

Fig.2: Proposed model of user registration process

C. information Matching

Among all information, matching is that the most significant a part of our model wherever our design has to verify the input file by examination with hold on information from the information. In the contingent method of this method is entirely designed in Fig.3. Stepwise procedure is narrated to a lower place

Step-1: the first step of knowledge matching starts with username and word, that stay encrypted exploitation the RSA algorithm. Encrypted information, then compared with the information. If the encrypted information accorded with the information, login gets the verification from the system and step a pair of begins. If not matched, then it showed with "Login Error".

Step-2: once prosperous verification, the user are going to be ready to choose future step. It consists of 2 choices wherever the user holds the privileges to pick out among these.

Option 1: This step works on users face recognition where the user's image are going to be captured by the device HD camera. during this step there ar five image samples can be taken from the user. Then Genetic algorithmic program is applied to the device as a kind of information for fitting with the information. If the data of the image is touched with the information, then the user gets the verified message to access the "Login" panel and if not, that's mean the user isn't verified that indicates a "Login Error".

Option 2: this selection can generate a QR code by utilizing the distinctive mackintosh address of the user's device.And it'll be given as a 3D barcode [8]. This barcode are matched with the registered barcode which keep on the information. If the info of barcode match to the information, then the user are ready to access "Login" panel and if the info of the barcode isn't matched, that's mean the user has not given the permission to access.

3. IMPLEMENTATION

In this half, we are going to establish however our prompt technique will discover out the user by exploitation 3 antecedently mentioned security technique. The implementation method will be shown for RSA, GA, and 3D QR Code Generator. Fig.4, Fig.5, & Fig.6, designates that however the implementation method is tested with real objects.

A. RSA formula

Generally, RSA uses 2 exponents, p, and q, where p is public and alphabetic character is bush key. Let the plaintext is M and C is ciphertext, then at secret writing [7]. $C = M^p \bmod n$ and

Decryption aspect become $M = C^q \bmod n$. Hither, this methodology used to generate the first layer system to urge this whole architecture. If user ready to log in with success, then the second layer are pictured, otherwise the error time can increase by showing a slip message. The second layer is predicated on user choice.

B. Genetic formula

A genetic formula is taken into account as heuristics based mostly search approach formula wherever chromosomes square measure treated as the main parameter. GA is employed to explore and optimize the problems solutions. Basic operations of GA square measure reproduction, crossover, and mutation. For a productive experiment choice of the input image from train info is stipulations wherever a private choice of tiny pel of that image is additionally obligatory. By applying crossover, it will ready to taper out the quantity of changes within the input check image comparison with train photos. Up next for minimum matching the procedure can calculate 10 generations of the image with matching and add up every quantity with Boolean (0 and 1) separation. Eventually, those pictures whose add value square measure decreased .
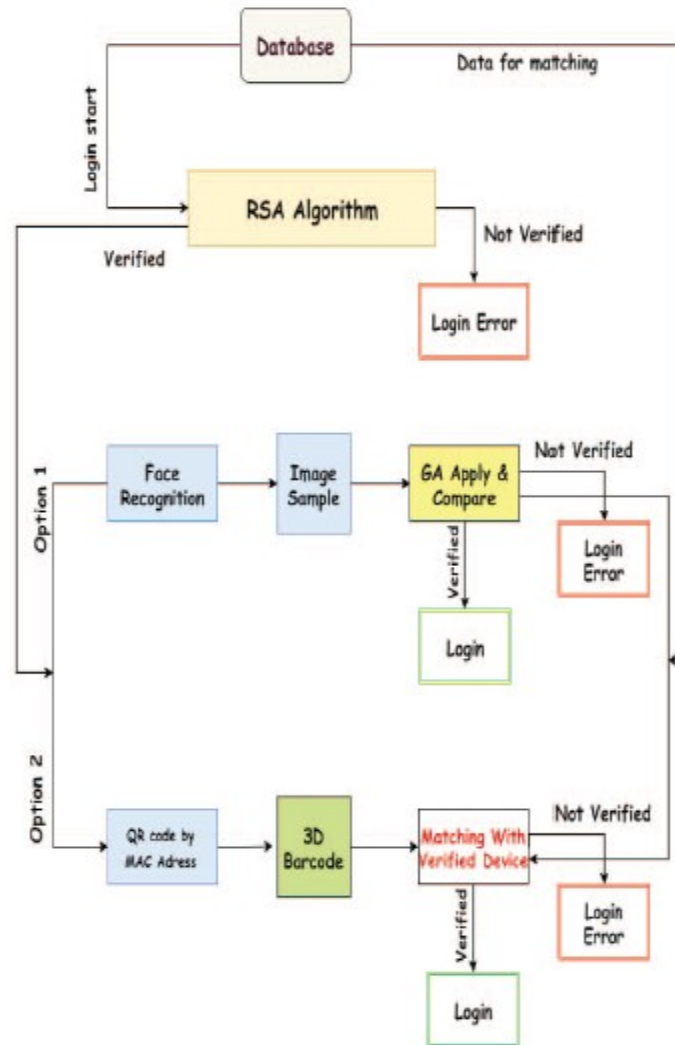
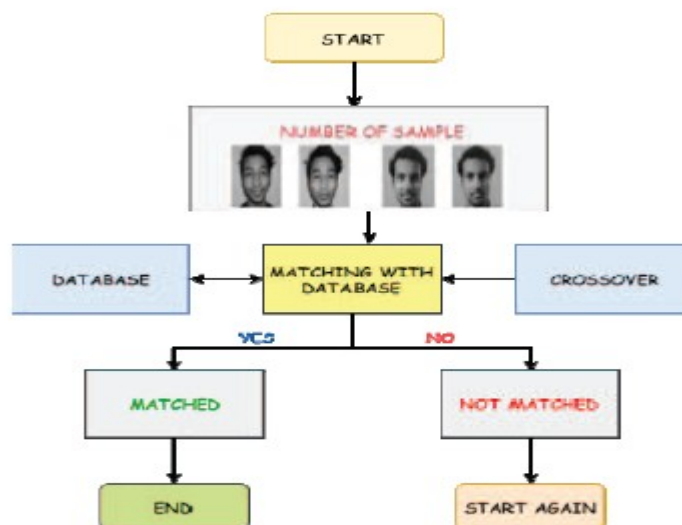Fig.3: Matching process of user data

Fig.4: A face matching procedure by using Genetic Algorithm

International Journal of Research
Available at https://edupediapublications.org/journals

e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 04
February 2018

Genetic rule consists essentially of creating a probe in the image of the article that almost all resembles AN conic of a proportional magnitude relation of one.5:1 [8]. The people, the ellipses ar written The sample code is given bellow:

Position of	X=	150	10010110
Position of	Y=	60	00111100
Ratio of	X=	95	01011111
Ratio of	Y=	80	01010000

In MATLAB the iteration is conducted by the sample image matrix binary values. Fig.5 depicts the whole procedure of face recognition mechanism using GA with some stepwise operations. Following steps (1-4) demonstrate how MATLAB is used to verify the face of users by comparing existing images with the database. For the successful experiment, we have utilized a personal database to successfully spot a face in MATLAB.

Step-1: Implementing and running the codes of GA to add some sample images for testing.

victimisation binary form, assumptive that every individual has four chromosomes, respectively: position X, position Y, the magnitude relation of X, and the ratio of Y.

Step-2: Bitmap (. bmp) image format is used in order to save samples for further use. Extract and upload process of samples are tracked by the database. These samples are employed to create a complete matrix for GA.

Step-3: Comparing two samples, namely sample1.bmp with sample2.bmp, the results show that mentioned samples are matched with each other. So the resolution designates the matching of experiment samples.

Step-4: Whenever the samples didn't match, results show the unsuccessful matching results.
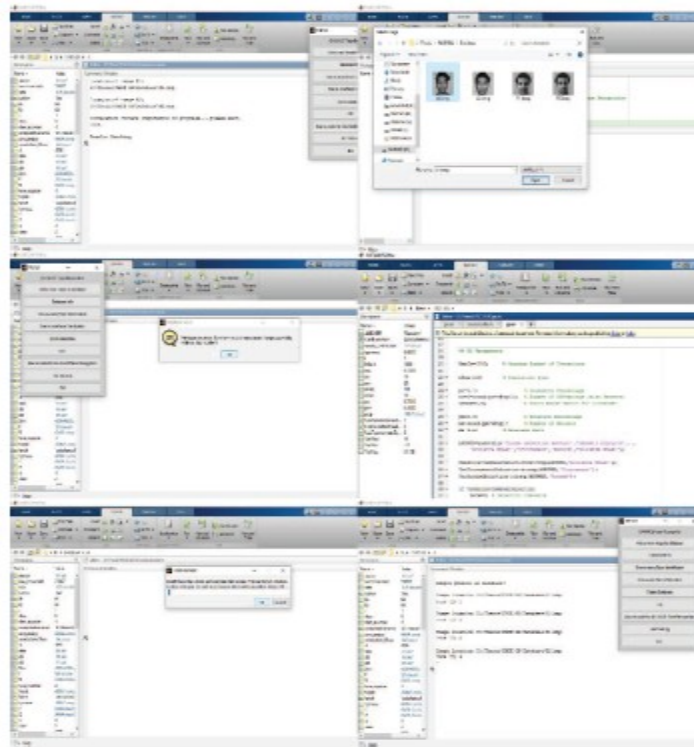
Fig.5: Implementation of face recognition in MATLAB

C. QR Code Generation

Another portion of the registration method relies on QR code generation. Generation of QR codes depends on the MAC address of individual devices. QR codes ar quickly arriving at high degrees of acceptance. a lot of and a lot of people adopt and use this technology a day. One of the reasons behind the zoom of the QR code is that it gains momentum as smartphone users grow across the globe and marketers use QR codes to succeed in mobile shoppers. [9] In this section, the device can got to register through an online page wherever that exact website can store the macintosh of that device for the cryptography functions. once more in verification section planned style system can shake off a barcode to registered users wherever the with success registered device needs to scan that code through a scanner. If that code matched with the login, then the user can take the winning verification otherwise specific section are going to be sealed. A complete illustration of the on top of discussion is delineate in Fig. 6. For our experiment, a macintosh address is applied to generate a QR code. Fig.6. Indicates the presence of macintosh ID 78: F7:BE:B7:83:57 in this specific QR code. After successful scanning of that QR code we've found the existence of that precise macintosh ID 78: F7:BE:B7:83:57 on it specific QR Code. winning execution of the QR code generation for users is clearly exhibited in Fig. 6.

Fig. 6: Bar Code generation procedure for users

4. EXPERIMENTAL RESULTS

Initially, we have a tendency to enforced RSA algorithmic program, Genetic Algorithm, and QR Code Generation technique for guaranteeing and enhancing higher security for cloud computing. The performance of the model depends on the values of encryption and cryptography cycle for every approach in terms of accuracy of the packages (kilobyte) transfer time. TABLE I show the time shrunken for each cryptography and decryption cycle with their average values for every planned technique.

Table.1: ACCURACY OF DIFFERENT ALGORITHMS

Steps	RSA Algorithm (ms)		Genetic Algorithm (ms)		QR Code (ms)		Average (%)
Encryption Cycle	84	75	98	92	34	31	84
Decryption Cycle	78	68	96	82	22	20	88
KB Transfer	768		928		104		

By analyzing the TABLE I, taken time by the Genetic Algorithm (GA) for each cryptography and secret writing cycle process indicates abundant higher comparison with the time taken by RSA algorithmic program and QR code.
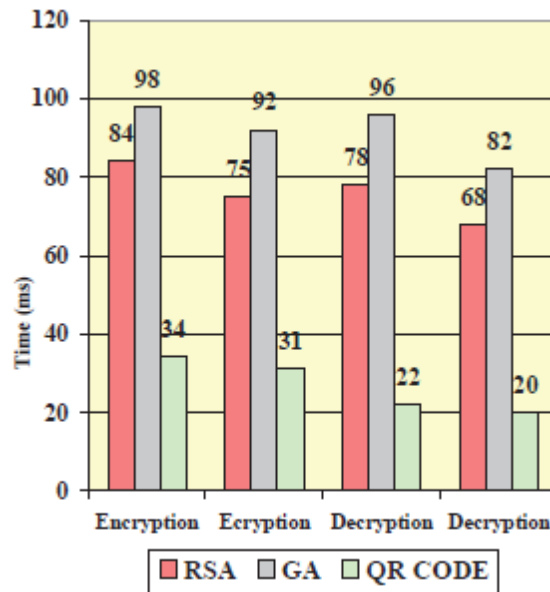
Fig. 7: The graphical representation of time required for encryption and decryption

Fig.7. Shows the graphical illustration of your time required for each encoding and decipherment cycle. For each algorithm calculation of your time limit and complexness are measured within the kind of Milliseconds (ms). Here from Fig.7 is visibly shown that within the initial try, the encoding method of RSA takes 84ms, whereas during a second try it takes 75ms. On the Contrary, Genetic formula takes 98ms and 96ms severally, for victorious encoding and QR Code takes 34ms and 31ms severally. once more within the segment of the decipherment method 78ms and 68ms is that the taken time for RSA, whereas the GA and QR take (96ms, 82ms) and (22ms, 20ms) correspondingly for decrypting information effectively.
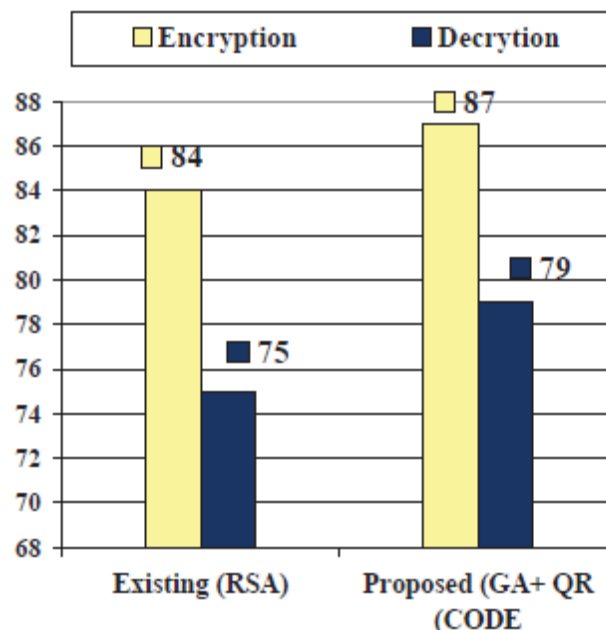
Fig. 8: Comparison of proposed methods with existing algorithm.

Fig.8. Exhibit the applied math comparison among projected (GA+QR CODE) technique with ancient existing RSA Algorithm. Here our projected methodology shows the upper accuracy of eighty seven as compared with RSA, that shows 84% of accuracy in terms of secret writing Cycle. Also for decryption cycle Fig.8 represents the upper accuracy of 79% in examination with the prevailing methodology of RSA that shows solely seventy fifth of accuracy. when an entire analysis of both Fig.7 and Fig.8 it is summarized that GA takes longer time compared with RSA whereas QR shows a minor time demand for secret writing and decipherment Cycle. Though GA takes longer time than RSA, still our projected method that may be a combination of (GA+QR Code) offer a higher security mechanism for cloud computing devices.

5. CONCLUSION

Enhance the protection of cloud computing with the combination of Genetic rule and QR Code. We have proposed a two-layer security mechanism that consists of Genetic rule for Face Recognition and fast Response (QR) technique for verification purpose. Currently, existing RSA approach is wide applied for the authentication purpose of cloud computing, devices that consist of the sole single layer, however our planned theme will supply the protection for the second level conjointly. Although our results don't seem to be nonetheless ok to be adopted in any commercial product for cloud computing devices, our approach still has vital prospective and blessings for further development. By examination the outcomes with existing we've got incontestible the efficiency of victimization the combination of each GA and QR. during this context of enhancing the protection of cloud computing victimization our suggested approach with existing one conjointly holds potential. So, we have a tendency to believe that the result of our planned model of providing a 2-Layer Security mechanism wherever the combination of GA and RA has been shown with Existing RSA model definitely make sure the superior security of cloud server. within the close to future, we are going to likewise attempt to implement Biometric Approach and assess the performance of whole approached model in terms of security sweetening of cloud computing.

REFERENCES

[1] R. L. Rivest , A. Shamir , L. Adleman, A method for obtaining digital signatures and public-key cryptosystems, Communications of the ACM, v.21 n.2, p.120-126, Feb. 1978 [doi>10.1145/359340.359342]

[2] Chun-Hung Lin and Ja-Ling Wu, "Automatic facial feature extraction by genetic algorithms," in IEEE Transactions on Image Processing, vol. 8, no. 6, pp. 834-845, Jun 1999.doi: 10.1109/83.766860.

[3] Yi-qiong Xu, Bi-cheng Li, and Bo Wang. 2004. Face Recognition by Fast Independent Component Analysis and Genetic Algorithm. In Proceedings of the The Fourth International Conference on Computer and Information Technology (CIT '04). IEEE Computer Society, Washington, DC, USA, 194-198K.

[4] Kris Antoni Hadiputra Nurwono and Raymondus Kosala. 2009. Color quick response code for mobile content distribution. In Proceedings of the 7th International Conference on Advances in Mobile Computing and Multimedia (MoMM '09). ACM, New York, NY, USA, 267-271. DOI=http://dx.doi.org/10.1145/1821748.1821799.

[5] David Gladstein; Ramakrishna Kakarala; Zachi Baharav"3D Barcodes: Theoretical Aspects and Practical Implementation" Proc. SPIE 9405, Image Processing: Machine Vision Applications VIII, 94050N (27 February 2015).

[6] Chu, Hung-Kuo, Chia-Sheng Chang, Ruen-Rone Lee, and Niloy J. Mitra. "Halftone QR codes." ACM Transactions on Graphics (TOG) 32, no. 6 (2013): 217.

[7] Rashmi Nigoti, Manoj Jhuria and Dr.Shailendra Singh, "A Survey of Cryptographic Algorithms for Cloud Computing" International Journal of Emerging Technologies in Computational and Applied Sciences, Vol. 4, pp.141-146, March-May 2013.

[8] F. Goudail, E. Lange, T. Iwamoto, K. Kyuma and N. Otsu, (1996)." Face recognition system using local autocorrelations and multiscale integration", IEEE Trans. PAMI, Vol.18, No. 10, 1024-1028.

[9] Sumit Tiwari "An Introduction To QR Code Technology" 2016 International Conference on Information Technology,Information Technology(ICIT),39-44