International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-8 Issue-10, August 2019

Secret Image Digitization Over Public Cloud Through Cbtv Based Image Fusion

Sangeeta Gupta, Ashwani Kumar

Abstract*: Data security in the modern world is a challenging aspect faced by common man in almost every field-either technical or non-technical. Particularly in Public Clouds where the data is openly available across the internet, customers are not much exposed to the working environment and the diverse spread of data across world wide geographic locations. Intruders attempt to misuse this data to serve their own commercial purpose. The government of India proposed NAD (National Academic Depository) which is a secure zone for people to deposit their valuable certificates rather than carrying to places. Towards this end, the goal of current work is to strengthen the security of certificates being loaded into the depositories by applying Image fusion technique through CBTV (Cloud Based Threshold Value). The proposed method gives a unique solution to prove authenticity of users by generating the secret image using image fusion technique integrated with public key infrastructure on the cloud prior to outsourcing. This is particularly useful to protect the patient health care reports to hide the disease description etc, which may otherwise have unintended consequences. The entire fusion is not disclosed at the cloud server end. The performance of the proposed approach, can be measure by calculating the robustness of the secret image (fused image) against different types of image processing attacks such as salt & pepper noise, Gaussian noise, JPEG compression, speckle noise, geometric noise etc. is calculated while stored at the cloud and effective results are achieved.

Keywords* : *Image fusion, Cloud computing, National academic Depository, Cloud based threshold value.

I. INTRODUCTION

UIDAI is a 12-digit unique identification number issued by the Indian government to every individual resident of India. It is used as a prime source of verification of an individual's identity and is a mandatory document to be produced when an individual want to avail benefits. It is also a source to reduce corruption in the country as every individual possess only one unique identity number. Even the National Academic Depository (NAD) relies on UIDAI to store all the academic awards.

Manuscript published on 30 August 2019.
***Correspondence Author(s)
Sangeeta Gupta, Dept. Of CSE, Chaitanya Bharathi Institute of Technology, Hyderabad, India.
Ashwani Kumar, Dept. Of CSE, Vardhaman College of Engineering, Hyderabad, India.

A. National Academic Depository (NAD)

Indian Higher Education System is a growing system with nearly 47 central universities, 365 state universities, 123 deemed universities, 269 private universities, issuing nearly 1.5 core Academic awards received by students per year.
NAD is the store house for all academic awards like certificates, degrees, marks sheets etc. duly digitized and lodged by academic institutions or eligibility assessment boards. It is a safe and secure online digital repository. It preserves the authenticity, integrity and confidentiality of the database [1].

NAD enables people to over-come long verification process which may end up in improper utilization of time and efforts. It also protects an individual from bearing the physical damage as they do not have to carry their most valuable documents to places. Security is achieved by individual authentication process through UIDAI number or NAD ID for the people who were unable to avail UIDAI services. By efficient utilization of the services offered by NAD students, parents, educational institutions, employees, corporate and government organizations can upload and retrieve the valuable certificates in a secure manner. There is no risk of theft, spoilage, hazard or tampering of confidential data deposited in NAD.

NAD Comprises of 2 inter operable digital depositories CVL (CDSL ventures Limited), NDML (NSDL Database Management Limited). These data stores en-sure the hardware, network facilities and software for secure functioning of NAD. University Grants Commission (UGC) on behalf of all the higher educational institutions is designated as an authority body for establishment of NAD. Users are given a choice to switch among the depositories if they are not satisfied with the services rendered. Interoperability enables the data across the depositories to be auto synced by making it easy for the user to operate with the same account which they created without having to make any changes.

B. CDSL Ventures Limits (CVL)

CVL is a subsidiary of Central Depository Services Limited (CDSL) which is a leading security depository in the country. It handles the work of customer record keeping for issuance of Know Your Client (KYC) acknowledgement to mutual fund investors. It first confirms the credentials of the investors and then only is-sues the KYC acknowledgement letter [2].

C. NSDL Database Management Limited (NDML)

NDML is a subsidiary of National Securities Depository Limited (NSDL). This group established Central Record Keeping Agency (CRA) for the new pension schemes, Unique Identification Authority of India (UIDAI) for implementation of UID mission in India. It has been involved in the projects of national significance being implemented for the first time by the government of India [3]. The above mentioned depositories are used by NAD to store customers confidential and most valuable certificates in a secure way with replication factor set i.e., if CVL is preferred by an individual to host data, then replicated copy of entire data in CVL is also stored across NDML and vice-versa. However, as UIDAI is the only source to confirm the authentication of an individual, there is a necessity to strengthen the security in the modern world. The need arises as intruders are misusing the data just by having access to the 12 digit UIDAI number through which the full residential address with pin code, contact details, date of birth etc are exposed to the intruders.

Hence, in this work, an attempt is made to strengthen the security of image being loaded into the depositories by applying Image fusion technique through CBTV (Cloud Based Threshold Value) rather than blindly uploading the UIDAI card. The proposed method gives a unique solution to prove authenticity of users by generating the secret image using image fusion technique integrated with public key infrastructure on the cloud prior to outsourcing. The entire fusion is not disclosed at the cloud server end. To evaluate the performance of the scheme, robustness of the secret image against different types of image processing attacks such as salt & paper noise, Gaussian noise, JPEG compression, speckle noise, geometric noise etc. is calculated while stored at the cloud and effective results are achieved.

The ideology of the paper of organized as follows: The First Section is Introduction that highlights the advancements made in technology in the modern India and need to safeguard secure data. The second section presents a background study. The third section throws a light on the proposed method with an architectural description to elaborate various modules used to design the work. The forth section presents an experimental evaluation to show the effectiveness of the proposed work and finally the fifth section concludes the work by igniting with the future directions.

s an International reputed journal that published research articles globally. All accepted papers should be formatted as per Journal Template. Be sure that Each author profile (min 100 word) along with photo should be included in the final paper/camera ready submission. It is be sure that contents of the paper are fine and satisfactory. Author (s) can make rectification in the final paper but after the final submission to the journal, rectification is not possible. In the formatted paper, volume no/ issue no will be in the right top corner of the paper. In the case of failure, the papers will be declined from the database of journal and publishing house. It is noted that: 1. Each author profile along with photo (min 100 word) has been included in the final paper. 2. Final paper is prepared as per journal the template. 3. Contents of the paper are fine and satisfactory. Author (s) can make rectification in the final paper but after the final submission to the journal, rectification is not possible.

II. RELATED WORK

The growth of cloud is increasing day by day we have witnessed it from the past decade. Now a day the services provided by the cloud are becoming available for the customers. The architecture of the public cloud computing consists of sharing different computing resources for customers. These sharing resources integrate different applications, software, and hardware platforms. The three vital services provided by the architectures of the cloud computing comprised i.e. Infrastructure as a Service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). Cloud is an emerging computing technique which makes use of internet and maintains data centre and servers. In cloud computing, cloud is nothing but a virtual resource [4]. It allows software developers to deploy different applications and services on the cloud these applications and services are shared by end user. [5], [6]. Kumar et al. [7-12] proposed different buyer seller watermarking protocol to provide secure and private transaction between the communicating parties.In general the benefits of the cloud are in the form of revolution, different serious issues and challenges are reported by cloud computing [13], [14]. These issues are connectivity and fault-tolerance capability adequate security etc [15]. At the other end, Watermarking techniques [16] are widely used to embed secret information inside a cover object while transmitting from sender to receiver pre-venting image distortion. Particularly Invisible watermarks form a key to preserve copyright protection, data hiding and authentication. A good number of watermarking algorithms [17] are in place. The most commonly used one is Least Significant Bit substitution technique which works efficiently for spatial data based images. However, if the nature of image is with respect to domains other than spatial, then LSB may not be effective.The other algorithm used is DCT Coefficient based watermarking [18] where either low or high frequency values chosen to embed data might lead to distortion, hence efforts are required to chose the frequency bands very carefully and it is a time consuming process. At the other end, there is Human Visual System (HVS) based watermarking [19] where the edge pixels are focused on to add the secret data. If translation of pixels take place, then the original data may be distorted in this technique. The loop holes identified using LSB, DCT and HVS techniques can be overcome Discrete wavelet transform (DWT) transforms [20] a discrete time signal to a discrete wavelet representation, which in turn projects a signal onto complete set of translated and dilation forms [21]. DWT is also integrated with cryptographic techniques to preserve copyright protection [22] to preserve anonymous communication between the buyers and sellers. The correlation coefficient of fusion image is calculating by passing the fusion image to low pass and high pass filters [23-24]. The disadvantage of wavelets it cannot record shapes and boundary edges of fusion images. Cloud is used for medical image processing to securely process the clinical decisions by authors in [25-26]. Hadoop system is used to improve the performance and availability and watermarking is used to ensure authentication. However, no methodology or experimental conduct is carried out to prove the effectiveness of the proposal.

Retrieval Number: J99390881019/19©BEIESP
DOI: 10.35940/ijitee.J9939.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)

III. PROPOSED APPROACH

Modern era is mostly prone to security threats with enormous technological advancements. Internet is a prime hub with added pros and cons where people search for anything and get the results. Even the different ways to eavesdrop any personal information are freely made available across the internet. Particularly in public cloud environment, though the service provider offers a limited amount of security to the data being stored, improper usage or lack of knowledge in that domain may lead to unintended consequences. For example in AWS server, if a user fails to have clarity or lack of knowledge in utilizing the resources in a proper way, the service provider may impose incidental charges.

Moving towards private cloud may offer the required level of securing confidential data from the intruders, but it is not a cost effective solution. This is because huge investments are required for the maintenance of infrastructure. Integration of public and private cloud offerings is a mix solution where if critical information is made available publicly then the secure data might fall into wrong hands. In order to prevent from such threats, it is essential for customers to have good exposure to the technology before trying to adopt the same and apply. This is however a time consuming process. Unique Identification Authority of India (UIDAI), is an agency to issue a 12-digit unique identification number i.e., Aadhar number initiated by the Indian government to every individual resident of India. It is used as a prime source of verification of an individual's identity and is a mandatory document to be produced when an individual want to avail benefits. It is also a source to reduce corruption in the country as every individual possess only one unique identity number. Even the National Academic Depository (NAD) relies on UIDAI to store all the academic awards.

UIDAI holders can show the printed QR code instead of revealing the 12-digit number. This QR code which is a form of bar code label contains machine read-able information. This code when scanned would read the non-sensitive user in-formation like name, date of birth, photo etc. But, this information exposed through the QR code is more than sufficient for the hackers to intrude and extract the other secret data. Towards this end, an attempt is made in this work to propose a system where the goal is to strengthen the security of certificates being loaded into the depositories like NAD by applying image fusion technique through CBTV (Cloud Based Threshold Value). The inputs are applied onto QR code, as an initial part of the work as it is a major source to preserve an individual's identity as used by NAD.

The proposed method gives a unique solution to prove authenticity of users by generating the secret image i.e. (fusion image in our case) in the form of a QR code using image fusion technique integrated with public key infrastructure on the cloud prior to outsourcing. The entire fusion is not disclosed at the cloud server end. This secret image (fusion image) now can be easily distributed over the public cloud data where this image can be assessed by the different parties for different purpose. To evaluate the performance of the scheme, robustness of the fusion image against different types of image processing attacks such as salt & paper noise, Gaussian noise, JPEG compression, speckle noise, geometric noise etc. is calculated while stored at the cloud and effective results are achieved. Figure 1 represents the system model implemented to carry out the proposed work.

The Algorithm for the proposed work is formulated as shown below:

Step1: An image of size 128×128 in the form of QR code is taken as input.

Step2: The concept of image fusion with 2- level of discrete wavelet transform is used to perform the following steps:

i) The QR code is decomposed using 2- DWT in an encrypted domain.

ii) Public key infrastructure (PKI) is then used for generating the secret fusion image.

Step 3: The threshold value of the fusion image QR code is calculated which helps to enhance the security of the fused image.

Step 4: The standard images along with their threshold values stored in the public cloud are compared with the threshold value of the fused image.

Step 5: If this threshold value is within the range of standard PSNR threshold value i.e. above 30db, then go to step 6.

Step 6: Generate the OTP.

Step7: User authentication successful else repeat steps 2 through 5 until a value within required range is obtained.

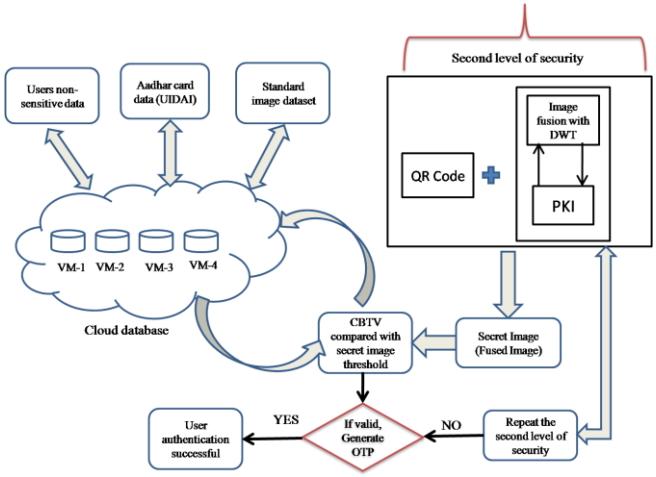

Fig. 1.Framework of digitization of Image fusion through CBTV scheme

IV. SYSTEM MODEL

The system model in this work includes four different types of entities: the QR image, Aadhar data, Standard image data set with cloud based threshold value (CBVT), and second level of security which comprises of formulating a secret fusion image by appending DWT with PKI watermarked inside the QR code. The first three entities are stored on public cloud using respectively virtual machines. In virtual machine 4, the threshold values for standard images are stored. This threshold value which is labeled as CBTV, is then compared with secret image (fusion image) threshold value to take a decision regarding the generation of OTP.

Published By:
Blue Eyes Intelligence Engineering
and Sciences Publication (BEIESP)

If the threshold value falls within the range i.e. PSNR value above 30db, then proceed towards generation of OTP. Otherwise, repeat the second level of security to extract valid threshold value. Once OTP is generated, the authentication from user end is marked to be successful.

V. RESULT AND DISCUSSION

In this section, result analysis of proposed scheme is presented on a variety of test QR code images of size 128 × 128 with the user non-sensitive information maintained at cloud VM. These images are depicted in Figure 2. An attempt is made to strengthen the security of UIDAI QR code being loaded into the depositories by applying Image fusion technique through CBTV (Cloud Based Threshold Value) rather than blindly uploading the UIDAI card. These secret fused images are thereafter distributed over the public cloud where they did not leak any sensitive information. Figure 2 (a-d) demonstrate the test image such as Lena image, Barbara image, Cameraman image and Pepper Image for producing the result. Figure 2 (e-h) shows the different types of QR code images. The visual quality of these fusion images (secret image) are calculated by imperceptibility and robustness metrics parameter. The perceptual quality of the fusion image is obtained with good resolution with respect to cover images and also no visual degradation was observed by the human visual system. Imperceptibility is measured by Peak Signal To Noise Ratio (PSNR) of the Fusion image and robustness is calculated by measuring the Normalized Correlation Coefficient (NCC) of the QR code Image. In figure 3 to 6 authors has demonstrated the entire process of image fusion graphically first a gray scale cover image of size 128 × 128 is taken then a binary QR code image is append into the cover image for generating the fusion image using DWT and PKI produces the secure secret fused image which is then stored into the public cloud. Author has taken different standard images with different types of QR codes for producing the secret images as shown in figure 3, 4, 5, 6. Author has successfully calculated the PSNR values for cover images and NCC values for QR code images as give in table 1 & 2.

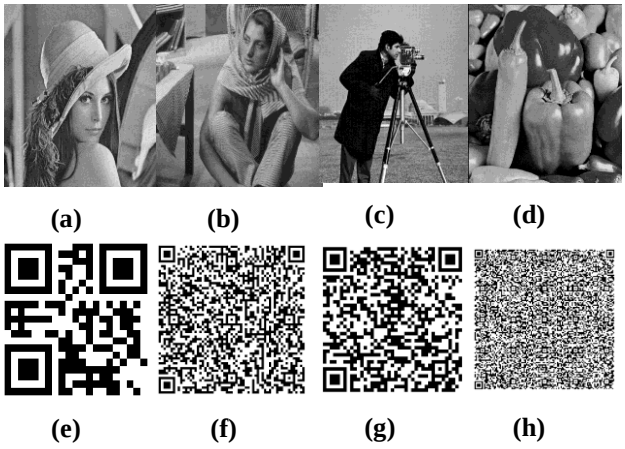

Fig. 2.The original images (a-d) with different types of QR code images (e-h) for image fusion processing.

Fig. 3.The original Lena images (a) The First QR code image (b) The cover fusion image stored on public cloud for further processing.

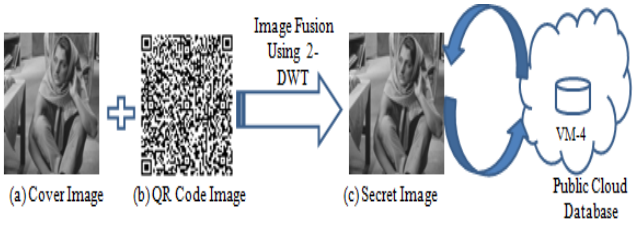

Fig. 4. The original Barbara image (a) The second QR code image (b) The cover fusion image stored on public cloud for further processing.

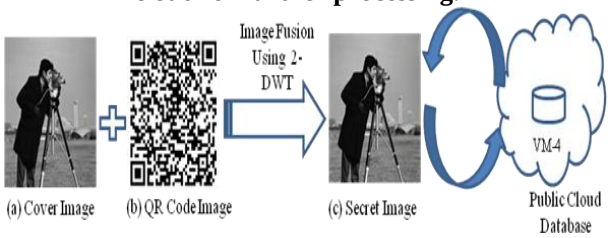

Fig. 5. The original Cameramen image (a) The Third QR code image (b) The cover fusion image stored on public cloud for further processing.

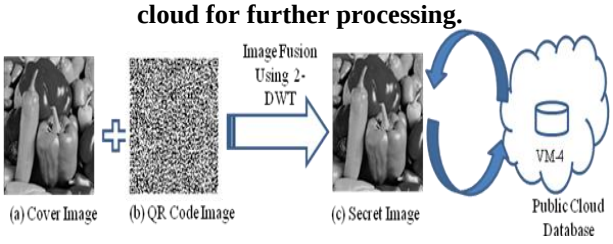

Fig. 6. The original pepper image (a) The Fourth QR code image (b) The cover fusion image stored on public cloud for further processing.

Table- I: PSNR values and NCC values for all cover images and QR image after attacks.

Images	Cameraman		Pepper	
Attacks	**PSNR**	**NCC**	**PSNR**	**NCC**
No Attacks	40.57	0.9231	40.57	0.9231
Salt & pepper Noise	32.45	0.6536	32.45	0.6536
Gaussian Noise	37.89	0.8754	37.89	0.8754
JPEG Compression	35.63	0.7971	35.63	0.7971
Speckle Noise	39.41	0.9013	39.41	0.9013

Table- 2: PSNR values and NCC values for all cover images and QR image after attacks.

Images	Lena		Barbara	
Attacks	**PSNR**	**NCC**	**PSNR**	**NCC**
No Attacks	43.59	0.9912	39.25	0.9153
Salt & pepper Noise	39.63	0.6338	35.10	0.4321
Gaussian Noise	39.72	0.6842	37.61	0.6541
JPEG Compression	41.01	0.8762	40.49	0.9653
Speckle Noise	35.93	0.5976	38.78	0.7432

In table 1 & 2 author have used various well known image processing attacks to check the validation of the proposed model the proposed scheme is tested under Salt & pepper noise, Gaussian noise, JPEG compression, Speckle noise etc. Author has used only few attacks for representing the result. The scheme performs well against the attacks especially in case of JPEG compression it gives good PSNR value above 40 and NCC is also above 0.8. The resolution of QR code images taken is of size 128 × 128 with the user's non-sensitive information maintained at cloud VM. A binary QR code image is appended into the cover image to generate the fused image. The proposed work is suitable for the images of range from 64 × 64 to 256 × 256. In future, the validity of the method can be strengthened by integrating other set of attacks in cloud environment. The various geometric distortion attacks such as cropping, rotation etc are not applied on the proposed work due to time constraint.

VI. CONCLUSION

In this paper, a secret image (fused image) digitization over public cloud model is presented which preserves the sensitive information of the users and avoids unauthorized access of the fusion image. The proposed method gives a unique solution to prove authenticity of users by generating the secret fused image using image fusion technique integrated with public key infrastructure. The proposed scheme performs well against the attacks especially in case of JPEG compression it gives good PSNR value above 40 and NCC is also above 0.8. Also, the resolution of QR code images taken is of size 128 × 128 with the user's non-sensitive information maintained at cloud VM. A binary QR code image is appended into the cover image to generate the fused image. However, the work is suitable for the images of ranging from 64 × 64 to 256 × 256. In future, there is a scope to use combined image fusion technique with different transforms for generating secret image. The imperceptibility can be further improved by robust technique. The effectiveness of the model can be further strengthened by adopting advanced security mechanisms.

REFERENCES

1. National Academic Depository (NAD), (2016, October 27) Available: http://nad.gov.in/
2. CVL is a subsidiary of Central Depository Services Limited (CDSL), which is a leading security depository in the country, (2017) Available: https://www.cvlindia.com
3. NDML is a subsidiary of National Securities Depository Limited (NSDL), Ministry of Human Resources Development and University Grants Commission, (2017, July) Available: https://nad.ndml.in
4. Armbrust M, Fox A, Griffith R, Joseph A.D, Katz R, Konwinski A, Lee G., Patterson D, Rabkin A, Stoica I, & Zaharia M, A view of cloud computing, In: Communications of the ACM, Vol. 53, No. 4, pp. 50–58, April, 2010.
5. Mukosi A, Mukwevho, & Celik, T. Toward A Smart Cloud: A Review Of Fault-Tolerance Methods In Cloud Systems, in IEEE Transactions on Services Computing, pp. 1-18, March 2018.
6. Z. Xia, X. Wang, L. Zhang, Z. Qin, X. Sun, and K. Ren, A privacy-preserving and copy–deterrence content-based image retrieval scheme in cloud computing, IEEE Trans. Inf. Forensics Security, Vol .11, No. 11, pp. 2594–2608, July 2016.
7. Kumar A., Paras Jain, Jabir Ali, Shrawan Kumar, G. John Samuel Babu, A Lightweight Buyer-Seller Watermarking Protocol Based On Time-Stamping and Composite Signal Representation", International Journal of Engineering & Technology, Vol. 7, No. 4.6, pp. 39-41, 2018.
8. Kumar A., Satya Prakesh Ghrera, & Vipin Tyagi, Modified Buyer Seller Watermarking Protocol based on Discrete Wavelet Transform and Principal Component Analysis, Indian Journal of Science and Technology, Vol. 8, No. 35, pp. 1-9, December 2015.
9. Kumar A., Satya Prakesh Ghrera, & Vipin Tyagi, A new and efficient buyer-seller digital Watermarking protocol using identity based technique for copyright protection, Third International Conference on Image Information Processing (ICIIP), Waknaghat, India, pp. 531-535, Dec. 2015.
10. Ashwani Kumar, Satya Prakesh Ghrera, & Vipin Tyagi, Implementation of wavelet based modified buyer-seller watermarking protocol, WSEAS Transactions On Signal Processing. Vol. 10, No. 1, pp. 212-220, 2014.
11. Kumar, Ashwani, Design of Secure Image Fusion Technique Using Cloud for Privacy-Preserving and Copyright Protection, International Journal of Cloud Applications and Computing (IJCAC), Vol. 9, No. 3, pp. 22-36, July-September 2019.
12. Ashwani Kumar, Sangeeta Gupta, A Secure Technique of Image Fusion Using Cloud Based Copyright Protection for Data Distribution, 2018 IEEE 8th International Advance Computing Conference (IACC), Greater Noida, India, pp. 14-15 Dec. 2018.
13. Aishwary K. Pandey, Priyanka Singh, Nishant Agarwal, Balasubramanian Raman, SecMed: A secure approach for proving rightful ownership of medical images in encrypted domain over cloud, In IEEE Conference on Multimedia Information Processing and Retrieval, Miami, FL, USA, pp. 390-395, April 2018.
14. Tchernykh, A., Schwiegelsohn, U., Talbi, E.g., & Babenko, M, Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability. Journal of Computational Science. JOCS, 581, pp.1-9, November 2016.
15. Gupta., S., & Narsimha., G, Secure Nosql for the social networking and e-commerce based big data applications deployed in cloud, International Journal of Cloud Application and Computing, Vol. 8, No. 2, pp. 113-129, April-June 2018.
16. Memon, N., & Wong, P.W, A buyer-seller watermarking protocol. IEEE Transactions on Image Processing, Vol. 10, No. 4, pp. 643–649, Apr 2001.
17. Subramanyam, A.V., Emmanuel, S., & Kankanhalli, M.S, Robust watermarking of compressed and encrypted jpeg2000 images, IEEE Transactions on Multimedia, Vol. 14, No. 4, pp. 703-716, December 2011.
18. Sverdlov, A., Dexter, S., & Eskicioglu, A.M, Robust DCT-SVD Domain Image Watermarking for Copyright Protection: Embedding Data in All Frequencies. 13th European Signal Processing Conference, Antalya, Turkey, pp.1-4, Sept. 2005.
19. Lai, C.C., Tsai, & C.C, Digital Image Watermarking Using Discrete Wavelet Transform and Singular Value Decomposition. IEEE Transactions on Instrumentation and Measurement, Vol. 59, No. 11, pp.3060-3063, September 2010.
20. Gupta S., & Bhattacharya., S, Invisible watermarking using a novel MRA based Image Fusion method. in proceeding of Annual IEEE India Conference (INDICON), Kochi, India, pp. 567-571, Dec. 2012.
21. Kumar A., Ghrera S.P., Tyagi V, A Comparison of Buyer-Seller Watermarking Protocol (BSWP) Based on Discrete Cosine Transform (DCT) and Discrete Wavelet Transform (DWT), In: Satapathy S., Govardhan A., Raju K., Mandal J. (eds) Emerging ICT for Bridging the Future - Proceedings of the 49th Annual Convention of the Computer Society of India (CSI) Volume 1. Advances in Intelligent Systems and Computing, vol 337. Springer, Cham, pp. 401-408, 2015.

22. Kumar., A., Ghrera., S.P., & Tyagi., V, An ID-based Secure and Flexible Buyer-seller Watermarking Protocol for Copyright Protection. Journal of Science & Technology Pertanika, Vol. 25, No. 1, pp. 57 – 76, January 2017.
23. Agarwal., J., & Beedi., S. S, Implementation of hybrid image fusion technique for feature enhancement in medical diagnosis, Human-centric Computing and Information Sciences, Vol. 5, No. 1, pp. 1-17, February 2015.
24. Yoonsuk Choi, Ershad Sharifahmadian, Shahram Latifi, Quality Assessment of Image Fusion methods in transform domain, International Journal on Information Theory (IJIT), Vol.3, No.1, pp. 7-18, January 2014.
25. M. Marwan, A. Kartit, and H. Ouahmane, Using cloud solution for medical image processing: Issues and implementation efforts, 3rd International Conference of Cloud Computing Technologies and Applications (CloudTech), Rabat, Morocco, pp. 1–7, Oct. 2017.
26. Zhan Qin, Jian Weng, Yong Cui, Kui Ren, Privacy-Preserving Image Processing in the Cloud In: IEEE Cloud Computing, Vol. 5,pp. 48-57, January 2018.

Retrieval Number: J99390881019/19©BEIESP
DOI: 10.35940/ijitee.J9939.0881019
Journal Website: www.ijitee.org

Published By:
Blue Eyes Intelligence Engineering and Sciences Publication (BEIESP)