Volume 7, Issue 1, January 2017 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Biometric Based Security Model for Cloud Computing Using Image Steganography

[1]A. Anuradha*, [2]Dr. Hardik B. Pandit
[1] L.J.Institute of Computer Applications, Ahmedabad, Gujarat, India
[2] Department of Computer Science, Sardar Patel University, Vallabh Vidyanagar, Gujarat, India

DOI: 10.23956/ijarcsse/V7I1/0114

Abstract— Information security has become an important issue, in the field of networking and in the emerging technologies like cloud computing. Cloud computing has become the modern alternative approach of sharing the computational resources around the globe. Though there is a hike in this trend, security of the outsourced data has become the most challenging issue. Thus securing of the data under communication as well as in the storage, is vital. Different approaches have been proposed by several researchers for enhancing the security thorough a combined technique of rich encryption and steganography. Also it has been accepted that Biometric identification is the best way of authenticating the owner of the data. For biometric identification finger prints, iris, palm, face and other personal information's can be used as unique ID's as a proof of authentication. The idea is to secure transformation and to maintenance of data. On the other side, image steganography has been proved to have better features in terms of security, capacity, robustness and integrity than the other types of information hiding techniques. In order to provide the security in the cloud computing it is must to have a clear understanding of the cloud computing, its environment, the architecture, various security concerns, the existing breach holes and an in-depth analysis of image steganography. Thus combining image steangography with biometrics and most advanced cryptographic and compression techniques, a more suitable and robust technique can be modelled for providing a better solution to the said problem.

Keywords— Cloud Computing, Information security, Cryptography, Watermarking, Steganography, biometric identification, real time image processing, finger print, encryption, compression

I. INTRODUCTION

The model proposed in this paper is baselined on cloud computing environment and its security issues. Thus to understand the security problem in the cloud and the solution model, it is must to have a better understanding of the cloud environment along with different techniques of information hiding [42], [44]. The said model is a biometric based image steganogarphy where finger print images have been incorporated for accurate authentication of the owner of the original data, along with maintaining the security of data during transmission.

A. Cloud Computing - The problem domain

Cloud computing is a service model providing access to a pool of resources like networks, servers, storage, applications and services on demand. On the other side security and vulnerabilities in the system has challenged the latest technology of computing [41], [45], [46]. Though cloud clients are keen to avail these advanced services, somewhere they are very much concerned for the data they are transmitting or storing in the cloud. Hence it is required to deal with the most important dimensions like security, availability and integrity of the data in this advanced computing environment [55]. The existing threats and vulnerabilities need to be resolved somehow, which are degrading the performance of the cloud service model [43], [48], [57]. The cloud architecture has to be studied well, the gaps need to be identified and effective mechanisms must be implemented to deal with such threats [47], [49], [52].

For proper maintenance of the secrecy of data, we have to be dependent on the third party, which is a tedious job and somewhat risky. It is really difficult to be completely dependent on them and to trust them [47]. Also the authentication of data is vital in this environment [61]. It would be a better approach, if a robust technique can be used, where the dependency on the third party service providers can be eliminated to a large extent.

B. An Overview of the solution

Image steganography has been proved to be the most robust technique of secret message passing. It is better than the techniques like cryptography, watermarking and other types of steganographic techniques like audio and text based steganography. But all these techniques have their own pros and cons as discussed in [115]. Cryptography converts the original data into ciphers making it difficult for the intruders to read the content. But steganography is somewhat a different concept, where the presence of data can not be known, which is secretly embedded as a part of the carrier signal [98], [99], [100], [101].

Watermarking is used as a part of authentication or ownership of the original data. Finger printing is the technique of using the characteristics of the source file in the form of a Meta file for distinguishing it from illegal sources [100]. Watermarking and fingerprinting has been used vigorously for authenticity. Steganography can also be implemented with watermarking, though both represent two different concepts. Steganography has two facets: one for protection against detection (Data hiding) and the other for protection against removal (Document marking). However for document marking both watermarking and finger printing can be used [101].

C. Image steganography - As an information security technique

Steganography is actually referred to "Covered writing". It is the concept of concealing text message, video or image in another file [8]. The concept of steganography is an old art and was a non-digital technique. Gradually it became digital with the revolution of IT. Steganography has been used as the technique of secret message passing and the robustness of the embedding process can be tested through steganalysis. The steganalysis aims at detecting the hidden messages in a cover [24]. The concept of steganalysis is very much similar to cryptanalysis, related to various image processing techniques like image filtering, image rotation, image cropping. Steganalysis can also be passive or active. The former one deal with covert message passing and the later applies the image processing techniques with the intention of destroying the secret message if any or to extract the secret message [113].

Among different steganographic techniques, image steganography has been considered as the most robust way of secret message transmission. Some of the important characteristics of image steganography that makes it so special among the other types are:

- **Undetectability** (To detect the presence of hidden data) [25]
- **Robustness** (To be safe from steganalysis attacks and different image transformations)
- **Capacity** (The amount of secret data that can be embedded in the image) [1],[27]
- **Amount of noise introduced** [14]
- **Security** (The extent to which data is safe from all aspects)
- **Invisibility** or **Perceptual transparency**: Based on the HVS system, depends on the distortion in the image leading to very less difference between the original and stego image [34]

Also different stegangraphic techniques used for secure transmission of data are [30]:

- Spatial Domain technique or Substitution technique
- Frequency Domain technique or Transform Domain technique
- Adaptive domain technique
- Spread Spectrum technique
- Distortion techniques
- Cover generation techniques
- Statistical techniques

All the above listed techniques work differently, giving importance to different aspects. Each follows a specific method of embedding the secret data. But the major domains of steganographic techniques are the spatial and frequency domains. However, the combination of these two named as the adaptive domain, is also another major technique of embedding secret data in an image, being considered as the third category. However a deeper study of all the techniques is essential for accomplishing the most appropriate method for fulfilling the important characteristics of the image steganography i.e. capability, robustness and undetectibility [8]. Thus a new technique can be developed considering all the specified techniques, with required characteristics.

For understanding the application domain of the proposed model being discussed in this paper, a detailed walkthrough of the existing applications is required. The existing applications of image steganography have been seen in a variety of areas [114]. To list down few of them are:

- Computer vision
- Remote sensing
- Feature Extraction
- Face Recognition
- Forecasting
- Optical Character Recognition
- Finger-Print Recognition System
- Medical image Processing

As information hiding in the cloud is the most recent and emerging area, for which different approaches have been suggested. Thus to provide a better solution, it is must to compare the existing techniques from all dimensions, so that a new fruitful technique can be invented, a robust model can be constructed possessing almost all the quality factors. The proposed model has been inclined towards providing security in this context.

D. Real-time image processing

The Kerckhoff's principle was proposed by a Dutch cryptographer Auguste Kerckhoffs, which states that, a cryptosystem must possess security, though everything about the system has been disclosed, except the key. The

principle is one of the basic principles of cryptography. With reference to this principle the source of images must be known to the public. Further the source of image taken is also very important .In the proposed model, the source of image will be from a mobile, representing the concept of real time image processing. Real time image processing supports freshly created images and does not refer to the images available in the web. Earlier it was done through cameras or related mechanisms, which have been challenged by mostly demanded equipments like mobiles. Mobiles are the instruments greatly used by all classes of public making it a convenient tool to be used for real time image processing [125].

In the name of social sites, people share lots of pictures in large volumes on a daily basis. So if such images can be used as a cover for transmitting the secret message, it can create less doubt on the part of the hackers. Also it provides less opportunity for them to manipulate the statistical characteristics of it, being taken from a dynamic source. In this way the steganalysis attacks can be avoided to some extent. The conventional pictures being used for steganography, though represents a robust technique but can never lead to uniqueness. So pictures taken from mobiles will definitely enhance the randomness as well as the robustness of the said technique.

E. Biometric based authentication

Based on the key to be used for doing the embedding in the cover image, image steganography can be : Pure steganography, Secret key steganography [24] or Public key steganography. In pure steganography no key is used. In Public key steganography a pair of keys is used: Public Key and Private Key. The former one is used for doing the embedding and the later for extracting the embedded message. But in secret key steganography, a secret key is shared between the sender and the receiver.

The proposed model, is based on the Secret key steganography (communication method is known but secret key is not known), which is different from Pure steganography (Communication method is not known), thus implementing the Kerckhoff's principle. To add value to the said model, a unique ID is generated from the finger print image. In addition to this, for a robust and unique embedding algorithm, deep study of the gaps in the human visual system has been considered to be significant.

Normally image processing is done for three different kinds of outputs [114]:

Case I: Output is an image

Case II: Output is some dimensions or measurement

Case III: Standard description of the image

However in the proposed model the image processing is done for unique ID generation from the fore finger print image, using some finger print device being taken on a real time basis. The ID generated thus, is used as the stego key in creating the stego image, preserving the robustness and uniqueness in the process of embedding. Also for the cover image generation, and thumb finger print image (for verifying the authenticity), mobile is used for getting the images on a dynamic basis. Since both the finger print image and the cover image are taken on a dynamic basis, the security of the system is enhanced.

II. NEED FOR THE PROPOSED MODEL

Cloud Computing is the most advanced platform where security is vital being a vast area. The review of literature done will be helpful for providing a secure band to the advanced technology. The positive aspect of the cloud computing is the global sharing of resources. Most of the companies are lessening their burden of managing their data, and with fewer expenses can use the remote resources available in the cloud to do so. However there is always the threat of security of their sensitive data in the cloud [61]. Thus security has been considered as the most challenging issue in this new era.

The cause of cloud environment threats is because of the existence of much vulnerability in the system. Various threats like side channel attack, denial of service attacks, authentication attack, and man in the middle attack along with some proposed solutions have been discussed and compared in terms of their strengths and weaknesses [41].

Out of some existing approaches, one way is to keep the data at multiple clouds for protecting the data from being attacked [54], [55], [56], [73], [74]. The next step that can be taken as a major of security is the encoding of data or sending the ciphers through the communication channels so that it can be protected from the hackers. Various issues in cloud computing like trust, privacy, security, ownership can be considered as the pivot elements of security, and the user must have the control over the encryption and decryption so as to boost their confidence [51].

Security can also be provided in the form of a model through the proper authentication, tokenisation for accessing the data, maintaining the log details of data item being accessed by stakeholders. Besides these, digital signatures can be considered as the essential element along with the encryption techniques (DES, ABE, RSA etc.)[53],[58],[59]. But in order to provide high security, the encryption techniques can be extended by increasing the encryption levels[62],[63] or cross breeding algorithms[66], and by providing a better way of authentication.

The data has been secured applying the technique of Digital watermarking. In [69], a combined approach of digital water marking based on discrete cosine transform (DCT) and discrete wavelet transform (DWT) has been proposed for a more effective watermarking. Identity based authentication has been considered for proving the ownership [55],[61].Digital signature, is a major identification technique [58] where the overhead of CA is there. But however biometric identification can be considered as the most unique method of identification [60], [64] and is more suitable than the conventional login id and password methods [68].

Steganography is the most advanced technique being proposed by most of the researchers currently along with high level of encryption techniques [62]. Cloud computing security can also be achieved by implementing techniques; those have been used for providing security in a network. Since the model is based on providing security, it can definitely work for cloud being an extended network. Thus the proposed research is based on the importance of cloud computing security, understanding the related causes and to go for a better solution through image steganography and unique authentication through fingerprint based identity.

III. PROPOSED MODEL

The proposed model is based on the real time image processing, where the cover image is generated using a mobile. As a part of authentication, the sender's thumb finger image is embedded in the cover. The thumb image will play the role of verifying the authenticity of the sender. Where as the fore finger image is used in generating the stego key to be used in the image steganography. To take finger print image, any finger print module that is reasonable in price can be used.

The process of embedding and extraction in the proposed model of image steganography can be described as follows:

A. For embedding

Before embedding, the secret message is first encrypted, and then compressed, using some existing standard techniques. Through encryption, the robustness of the secret transmission is enhanced, and through compression, the message size is reduced. Before embedding, the data is encrypted as this process, not only minimises the amount of information to be embedded but also generate more irregular data providing more or almost double security for the data to be transmitted.

The Kerckhoff's principle (Secret key steganogrphy) of maintaining the secrecy even if the embedding algorithm is made available except the secret key is implemented. The model uses thumb finger image and fore finger image as the cover and stego key respectively. For embedding the secret data, a robust algorithm has been designed. Thus three different algorithms are used. One for embedding the thumb finger print image into the cover, one for generating the unique ID: to be used as the stego key, and the last one for embedding the secret data into the cover image.

Among different techniques of steganography, frequency domain based steganography is the robust one. Also among different frequency based techniques, performance of DWT technique is superior to DCT, FFT etc. Thus during embedding, the image is converted into DWT based frequency domain for improved results. The model for embedding the secret message can be represented as in [Fig. 1]:

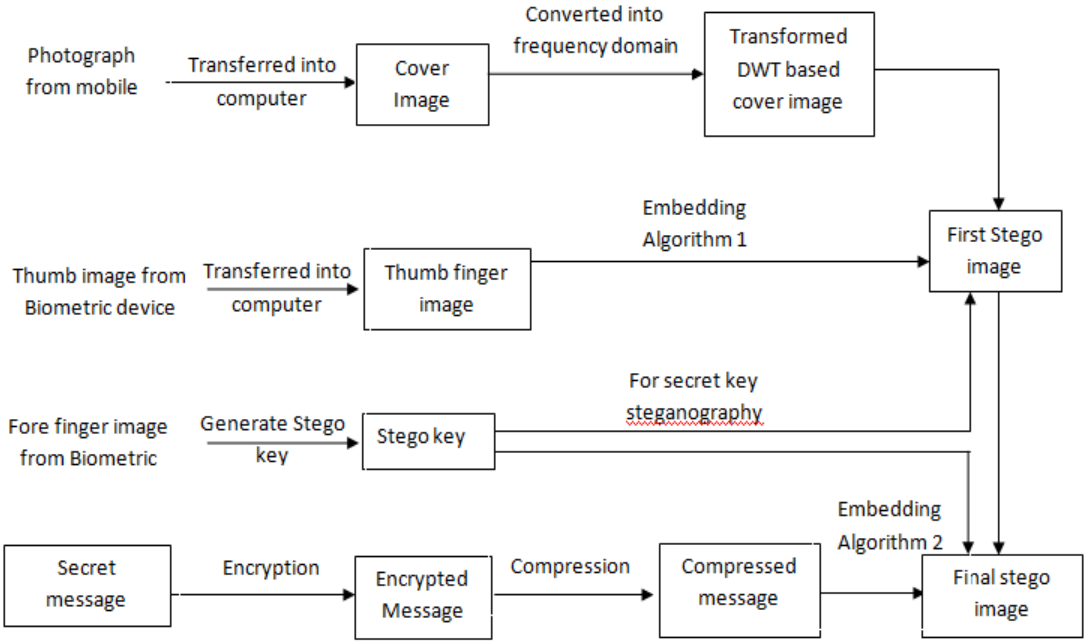

Fig. 1 : Block diagram for embedding

B. For Extraction

In the reverse process of removing the secret message, the receiver first extracts the finger print image. A database containing the expected sender's finger prints and their corresponding unique ID's is maintained. On receiving the final stego image, the extracted finger print's unique ID is matched with that of the ID stored in the DB. If any matching is found, i.e. if it matches with one of the intended senders ID's, then only the reverse process of embedding algorithm is applied to get back the compressed and encrypted message.

The idea behind the model is that, first the authentication is verified. If it succeeds then only the intended message is retrieved. Therefore, by applying the reverse process, the original decrypted message is digged out. The extraction model can be represented as in [Fig. 2]:

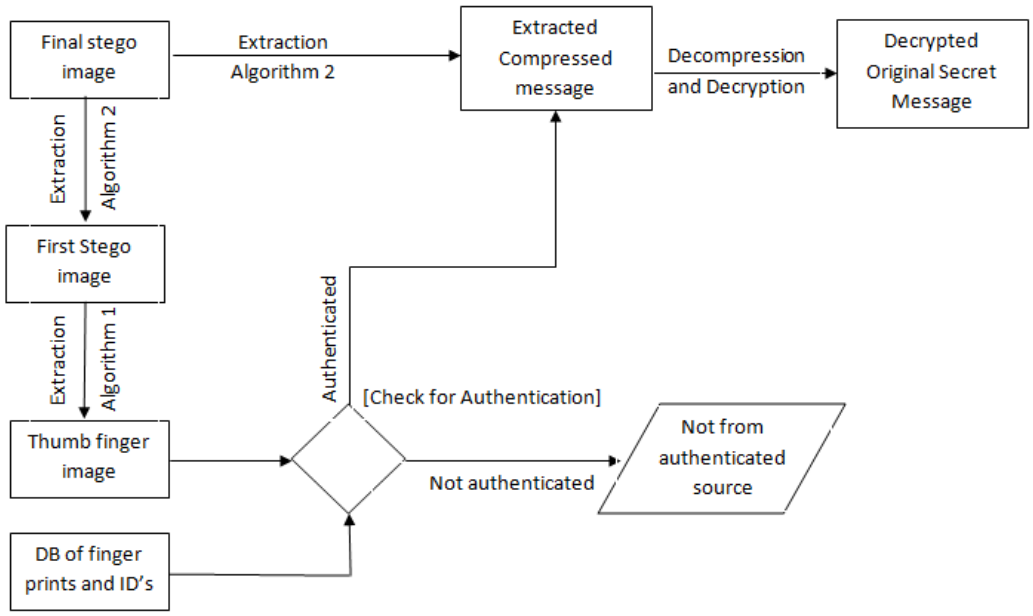

Fig. 2 : Block diagram for Extraction

C. Proposed algorithm

1) Sender side: The algorithm includes

- Transform the photograph from the mobile in the JPEG format into the computer, to be used as the cover image.
- Generate the DWT version of the cover image.
- Capture the Thumb finger image in JPEG format using some digital finger printing device, to be used for authentication.
- Capture the Fore finger image in JPEG format using some digital finger printing device.
- Generate Unique ID from the Fore finger image, to be used as the stego key.
- Merge the thumb finger image with the cover image to form the first stego image using the stego key.
- Encrypt the secret data to be transmitted using some standard encryption.
- Compress the encrypted message to reduce its size, using some standard compression technique.
- Embed the secret message in the first stego image using the stego key forming the second stego image.
- Transmit the second stego image is in the cloud.

2) Receiver side: The algorithm includes

- Receive the final stego image being sent from the sender.
- Remove the original secret message from it using the reverse process of embedding, thus separating the first stego image and original message (in the compressed and encrypted form).
- Extract the thumb finger image from the first stego image by applying the reverse process of embedding done at the sender side.
- Compare the thumb finger image ID with the DB of finger print ID's being maintained at the receiver side.
- If a match is found then the received message is considered to be from a legitimate sender and the original message is extracted through decryption, followed by decompression.
- If no match is found, it is understood that the message is not from a legitimate user and no extraction is done.

IV. CONCLUSION

Image Steganography has been used vigorously, and researchers have come with a variety of embedding techniques for secret transmission of data. Though researchers spoke on biometric based algorithms, used for skin tone detection for embedding the secret data within skin regions [95] or for medical related applications, but nobody discussed on its use as a combined technique of secret message passing and for authentication proof, which is the baseline of the proposed model. Therefore in the proposed model, the concept of biometrics has been used for identifying the legitimate senders and for message embedding. A robust algorithm based on unique stego key generated from fore finger print image is employed. The speciality of finger prints is that they can uniquely identify any person. Even two twins can not have the same finger print impressions. Obviously, the ID generated from the finger print will also be unique, making the message transmission more secure. Thus the model is not only capable of maintaining the uniqueness but also strong enough against steganalysis attacks.

REFERENCES

[1] Abbas Cheddad, Joan Condell, Kevin Curran and Paul Mc Kevitt, "Biometric Inspired Digital Image Steganography",*15th Annual IEEE International Conference and Workshop on the Engineering of Computer Based Systems*, 978-0-7695-3141-0/08 $25.00 © 2008 IEEE, DOI 10.11.1109/ECBS.2008.11.

[2] Snehal O. Mundhada, V.K.Shandilya, "Spatial and Transform Domain Techniques for Image Enhancement", *International Journal of Engineering Science and Innovative Technology (IJESIT)*, ISSN:2319-5967, Volume 1, Issue 2, November 2012.

[3] Ms.G.S.Sravanthi, Mrs.B.Sunitha Devi, S.M.Riyazoddin & M.Janga Reddy, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", *Global Journal of Computer Science and Technology Graphics & Vision*, Online ISSN: 0975-4172 & Print ISSN: 0975-4350, Volume 12 Issue 15 Version 1.0 Year 2012.

[4] Champakamala .B.S, Padmini.K, Radhika .D. K Asst Professors, "Least Significant Bit algorithm for image steganography", *International Journal of Advanced Computer Technology (IJACT)*, ISSN:2319-7900, VOLUME 3, NUMBER 4.

[5] Prof. Samir Kumar Bandyopadhyay, Indra Kanta Maitra, "An Application of Palette Based Steganography", *International Journal of Computer Applications (0975 – 8887)* Volume 6– No.4, September 2010.

[6] V.M. Potdar, S.Han an E.Chang, "Finterprinted secret sharing steganography for robustness against image cropping attacks", *Preceding of IEEE 3rd International Conference on Industrial Informatics (INDIN)*, Perth, Australia, 10-12 August 2005, pp. 717-724.

[7] Z. Li,.X. Chen, X. Pan and X. Zeng, "Lossless data hiding scheme base on adjacent pixel difference", *Proceeding of the International Conference on Computer Engineering and Technology*, 2009,pp. 588-592.

[8] A.Cheddad, J. Condell, K. Curran and P. Mc Kevitt,"Digital Image Steganography: Survey and Analyses of Current Methods", Signal Processing, Volume 90, Issue 3, March 2010, Pages 727-752.

[9] Abbas Cheda, Joan Condell, Kevin Curran and Paul Mc Kevitt, "A Secure and Improved Self-Embedding Algorithm To Combat digital Document Forgery".

[10] Akanksha Kaushal, Vineeta Chaudhary, "Secured Image Steganography using Different Transform Domain", *International Journal of Computer Applications (0975-8887)*, Volume 77 – No.2, September 2013.

[11] Champakamala . B.S., Padmini. K. Radhika .D. K , "Least signficant Bit algorithm for image steganogarphy ", *International Journal of Advance Computer Technology*, Volume 3, Number4.

[12] Dr. Mahesh Kumar, Munesh Yadav, "Image Steganography Using Frequency Domain", *International Journal of Science & Technology Research*, ISSN 2277-8616, Volume3, Issue9, September 2014.

[13] Johnson, N.F. & Jaljodia, S., "Steganalysis of Image Created Using Current Steganography Software", Proceeding of the 2nd Information Hiding Workshop, April.

[14] Ms.G.S. Sravanti, Mrs. B. Sunitha Devi, S.M. Riyazoddin & M. Janga Reddy, "A Spatial Domain Image Steganography Technique Based on Plane Bit Substitution Method", CMR Institute of Technolog, Hyderabad, Andhra Pradesh, India.

[15] Paul Alvarez, "Using Extended File Information (EXIF) File Headers in Digital Evidence Analysis", *International Journal of Digital Evidence*, winter 2004, Volume 2, Issue 3.

[16] Andreas Westfeld, "F5 – A Steganographic Algorithm High Capacity Despite Better Steganalysis", I.S. Moskowitz (Ed.): IH 2001, LNCS 2137, pp. 289-302, 2001. © Springer – Verlag Berlin Heidelberg 2001.

[17] Andreas Westfeld, "Detecting Low Embedding Rates", F.A.P. Petitcolas (Ed.): IH 2002,

[18] LNCS 2578, pp. 324-339, 2003. © Springer – Verlag Berlin Heidelberg 2003.Andrew D. Ker, "Improved Detection of LSB Steganography in Grayscale Images", J. Fridrich (Ed.): IH 2004, LNCS 3200, pp. 97-115, 2004. © Springer – Verlag Berlin Heidelberg 2004.

[19] Mehdi Kharrazi, Husrev T. Sencar, Nasir Memon, "Performance study of common image steganography and steganalysis techniques", *Journal of Electronic imaging* ,Vol. 15(4), 041104-1 (Oct-Dec 2006).

[20] Kaushal Solanki, Anindya Sarkar, B.S. Manjunath, "YASS : Yet another Steganographic Scheme that Resists Blind Steganalysis".

[21] K.B.Raja, C.R.Chowdary, Venugopal K R, L.M. Patnaik, "A Secure Image steganography using LSB, DCT and Compression Techniques on Raw Images", 0-7803-9588-3/05/$20.00©2005 IEEE.

[22] Jiri Fridrich, Center for intelligent Systems, SUNY Binghampton,"A New Steganographic Method for Palette-Based Images".

[23] Jian Zhao, Eckhard Koch, "Embedding Robust Labels into images for Copyright Protection", In Proc. of the Int. Congress on Intellectual Property Rights for Spcialized Information, Knowledge and New Technologies, Vienna, August 1995.

[24] Jessica Fridrich, Miroslav Goljan, Dorin Hogea, David Soukal, "Quantitative Steganalysis of digital images : estimating the secret message length", Multimedia Systems © Springer-Verlag 2003, Digital Object Identifier (DOI) 10.1007/s00530-003-0100-9.

[25] Jessica Fridrich, Miroslav Goljan, "On Estimation of Secret Message Length in LSB Steganography in Spatial Domain", Department of Electrical and Computer Engineering, SUNY Binghamton, NY 13902-6000.

[26] Jessica Fridrich, Miroslav Goljan, Rui Du, "Reliable Detection of LSB Steganography in color and Grayscale Images".

[27] Jarno Mikikainen, "LSB Matching Revisited", *IEEE SIGNAL PROCESSING LETTERS*, Vol.13, No. 5. May 2006, 1070-9908/$20.00 © IEEE.

[28] D.C. Wu and W.H. Tsai, "A Steganographic method for images by pixel-value differencing", Pattern Recognition Letters, Vol. 24, no. 9-10, pp 1613-1626, 2003.

[29] Hsien-Chu Wu, Na-I Wu, Chwei-Shyong Tsai, Min-Shiang Hwang, "An Image Steganographic Sheme Based on Pixel-Value Differencing and LSB Replacement Methods", Department of Management Information System, November 7,2004.

[30] H.S. Manjunatha Reddy, K B Raja, "High Capacity and Security Steganography using discrete wavelet transform", *International Journal of Computer Science and Security (IJCSS)*, Volume(3), Issue(6).

[31] C.P. Sumathi, T. Santanam, G.Umamaheswari, "A Study of Various Steganographic Techniques Used for Information Hiding", *International Journal of Computer Science & Engineering Survey (IJCSES)*, Vol.4, No.6. December 2013.

[32] Seyyed Amin Seyyedi, Nick Ivanov, "An Adaptive Steganographic method in frequency domain based on statistical metrics of image", *Internantional journal of Cyber-Security and Digital Forensics (IJCSDF)*, Vol.3, No.1, Apr - 2014.

[33] Shikha Sharda, Sumit Budhiraja, "Image steganography : A Review", *International Journal of Emerging Technology and Advanced Engineering*, ISSN 2250-2459, ISO 9001:2008 Certified Journal, Volume 3, Issue 1, January 2013.

[34] Zaidoon Kh. AL-Ani, A. A. Zaidan, B.B. Zaidan and Hamdan.O.Alanazi, "Overview: Main Fundamentals for Steganography", *Journal of Computing*, ISSN 2151-9617, Volume 2, Issue 3, March 2010.

[35] Rengarajan Amirtharajan, Kiaohua Qin and John Bosco Balaguru Rayappan, "Random Image Steganography and Steganalysi : Present Status and Future Directions", *Information Technology Journal 11 (5)* : 566-576, 2012.

[36] Lip Yee Por, Delina Beh, Tan Fong Ang and Sim Ying Ong, "An Enhanced Mechanism for Image Steganography Using Sequential Colour Cycle Algorithm", *The International Arab Journal of Information Technology*, Vol.10, No.1, January 2013.

[37] G. Manikandan, M.Kmarasan and N.Sairam, "A New Approach for Secure Data Transfer based on Wavelet Transform", *International Journal of Network Security*, Vol. 15, No.1. PP.88-94, Jan 2013.

[38] Regunathan Radhekrishnan, Mehdi Kharrazi and Nazir Menon, "Data Masking: A New Approach for Steganography", *Journal of VLSI Signal Processing* 41, 293-303, 2005.

[39] R. Amirtharajan, John Bosco Balaguru Rayappan, "Steganography – Time to Time: A Review", Research Journal of Information Technology – February 2013, Resarchgate.

[40] S. K. Muttoo, Sushil Kumar, "A Multilayered Secure, Robust and High Capacity Image Steganography Algorithm", *World of Computer Science and Information Technology Journal (WCSIT)*, ISSN: 2221-0741, Vol.1, No.6,239-246, 2011.

[41] KallimullahLone, Md. Ataullah, "A Review on Cloud Computing Privacy Solutions", *International Journal of Advanced Research in Computer Science and Software Engineering*, ISSN: 2277 128X, Volume 3, Issue 2, February 2013.

[42] G.Kalpana, P.V. Kumar and R.V.Krishnaiah, "A brief Survey on Security Issues in Cloud and its Service models", *International Journal of Advanced Research in Computer and Communication Engineering* ,Vol. 4,Issue 6, June 2015.

[43] Devanshu Tiwari, Assit. Prof. Damodar Tiwari, "A survey of cloud computing security threats", *International Conference on Cloud, Big Data and Trust 2013*, Nov 13-15, RGPV.

[44] S.Sudha, V.Madhu, Viswanatham, "Addressing security and privacy issues in cloud computing", Issn: 1992-8645, E-Issn: 1817-3195, Vol. 48 no.2, 20th february 2013.

[45] Keiko Hashizume,David G Rosado,Eduardo Fernández-Medina and Eduardo B Fernandez, "An analysis of security issues for cloud computing", Hashizume et al. *Journal of Internet Services and Applications 2013*, 4:5.

[46] Vishnu Patidar, Makhan Kumbhkar, "Analysis of Cloud Computing Security Issues in Software as a Service", *International Journal of Scientific Research in Computer Science and Engineering*, ISSN: 2320-7639, Volume-2, Issue-3 30 Jun 2014.

[47] Abraham E. Eviwiekpaefe, Fiyinfoluwa Ajakaiye, "The trend and challenges of cloud computing: a literature review", *International Letters of Social and Humanistic Sciences* Vol. 16 (2014) pp 13-20.

[48] Dr.P.K.Rai, , R.K.Bunkar, "Study of Security Risk and Vulnerabilities of Cloud Computing",*International Journal of Computer Science and Mobile Computing (IJCSMC)*, ISSN 2320–088X, Vol.3, Issue. 2, February 2014, pg.490 – 496.

[49] Ms. Disha H. Parekh, Dr. R. Sridaran, "An Analysis of Security Challenges in Cloud Computing",IJACSA) *International Journal of Advanced Computer Science and Applications*,Vol. 4, No.1, 2013.

[50] W.Sharon Inbarani, C.Kumar Charlie Paul, W.Andrew Jerome Jeevakumar, "A Survey on Security Threats and Vulnerabilities In Cloud Computing", ISSN 2229-5518, International *Journal of Scientific & Engineering Research*, Volume 4, Issue 3, March -2013.

[51] Mohit Marwaha , Rajeev Bedi, "Applying Encryption Algorithm for Data Security and Privacy in Cloud Computing", *IJCSI International Journal of Computer Science Issues* ,ISSN (Print): 1694-0784 | ISSN (Online): 1694-0814, Vol. 10, Issue 1, No 1, January 2013.

[52] Miss. Pallavi A. Patil, Prof. K. G. Bagde, "Cloud Computing and Faults in Cloud Computing", *International Journal of Computer Science and Mobile Computing(IJCSMC)*, ISSN 2320–088X, Vol. 3, Issue. 5, May 2014, pg.415 – 42.

[53] R. Bala Chandar, M. S. Kavitha, and K. Seenivasan, "a proficient model for high end security in cloud computing", *ictact journal on soft computing*, january 2014, volume: 04, issue: 02.

[54] Mr.K.Sriram,Ms.N.Radhika, "a scalable and secure sharing of phr in cloud computing",*International Journal of Computer Science and Mobile Applications*, ISSN: 2321-8363, Vol.2 Issue. 3, March- 2014, pg.35-41.

[55] V. Spoorthy, M. Mamatha, B. Santhosh Kumar, "A Survey on Data Storage and Security in Cloud Computing", *International Journal of Computer Science and Mobile Computing*, ISSN 2320–088X, Vol. 3, Issue. 6, June 2014, pg.306 – 313.

[56] Ms. Mayuri R. Gawande, Mr. Arvind S. Kapse, "Analysis of Data Confidentiality Techniques in Cloud Computing", *Ijcsmc*, issn 2320–088x,Vol. 3, Issue. 3, March 2014, pg.169 – 175.

[57] Swapna Lia Anil, Roshni Thanka, "A Survey on Security of Data outsourcing in Cloud", ISSN 2250-3153 ,*International Journal of Scientific and Research Publications*, Volume 3, Issue 2, February 2013.

[58] Parul Mukhi,Bhawna Chauhan, "Survey on triple system security in cloud computing", ijcsmc, ISSN : 2320–088x ,Vol. 3, Issue. 4, April 2014, pg.1108 – 1115.

[59] Ravi j. Khimani, nishant s. Sanghani, asst. Prof. K.k. sutaria, "ameliorate security policy using mediated rsa and identity based cryptography in cloud computing".

[60] Muhammad Adeel Javaid, "Cloud Computing Security and Privacy", *Computer Science and Information Technology 2(5)*: 219-231, 2014.

[61] Monjur Ahmed and Mohammad Ashraf Hossain, "Cloud computing and security issues in the cloud",*International Journal of Network Security & Its Applications (IJNSA)*, Vol.6, No.1, January 2014.

[62] Nouf A. Al-Otaibi, Adnan A. Gutub, "2-Leyer Security System for Hiding Sensitive Text Data on Personal Computers", *Lecture Notes on Information Theory* Vol. 2, No. 2, June 2014.

[63] Aparjita Sidhu,and Rajiv Mahajan, "Enhancing security in cloud computing structure by hybrid encryption", *International Journal of Recent Scientific Research*, ISSN: 0976-3031,Vol. 5, Issue, 1, pp.128-132, January, 2014.

[64] Varsha Yadav, Preeti Aggarwaal, "A Survey on Security in Cloud Computing", *IJCSMC*, ISSN : 2320–088X , Vol. 3, Issue. 4, April 2014, pg.509 – 513.

[65] Karun Handa, Uma Singh, "Data Security in Cloud Computing using Encryption and Steganography", *IJCSMC*, ISSN 2320–088X ,Vol. 4, Issue. 5, May 2015, pg.786 – 791.

[66] Rajesh Kumar, A.J. Singh, "Understanding Steganography over Cryptography and Various Steganography Techniques", *IJCSMC*, ISSN 2320–088X, Vol. 4, Issue. 3, March 2015, pg.253 – 258.

[67] Ch. Anjani Kumar, and K. Subba Rao,"Usage of Multiple Clouds to increase Security in Cloud Computing", International Journal of Computer Sciences and Engineering,E-ISSN: 2347-2693, May 2014, Volume-2,Issue- 5.

[68] Mayron, LM, "Biometric Authentication on Mobile Devices", *IEEE Computer Society*, IISN: 1540- 7993, May-June 2015.

[69] Deepakshi Bhardwaj, Ms.Nutan , "Hiding of Image Data behind a Colored Image Using Advanced DWT Method", ISSN: 2277 128X, Volume 4, Issue 5, May 2014.

[70] Hamad Naeem, Jun Sang, Waqar Ali Abro, Adeel Khalid, Muhammad Rashid Naeem, Adeel Akbar Memon, Saad Tanvir, "Message Encryption by Processing Image Using Pseudo Random Key Streams Generation", *International Journal of Computer Trends and Technology (IJCTT)* – volume 20 Number 2 Feb 2015.

[71] Richa Dubey, Apurva Saxena, Sunita Gond, "An Innovative Data Security Techniques Using Cryptography and Steganographic Techniques", (IJCSIT) *International Journal of Computer Science and Information Technologies*, ISSN: 0975-9646, Vol. 6 (3) , 2015, 2175-2182.

[72] Sudipta Sahana, MadhusreeMajumdar, Shiladitya Bose, AnayGhoshal, "Security Enhancement Approach For Data Transfer Using Elliptic Curve Cryptography And Image Steganography", *International Journal of Advanced Research in Computer and Communication Engineering*, ISSN (Online) 2278-1021 ISSN (Print) 2319-5940 Vol. 4, Issue 4, April 2015.

[73] Sasikumar Gurumurthy, T. Niranjan Babu, G. Siva Shankar, "An Approach for Security and Privacy Enhancing by Making Use of Distinct Clouds", *International Journal of Soft Computing and Engineering (IJSCE)* ISSN: 2231-2307, Volume-4, Issue-2, May 2014.

[74] Prof. J. M. Patil, Ms. B. S. Sonune, "Data protection over multiple clouds using encryption technique", *International Journal of Modern Trends in Engineering and Research*, e-ISSN No.:2349- 9745, Date: 2-4 July, 2015.

[75] Hardikkumar V. Desai, "Steganography, Cryptography, Watermarking: A Comparative Study", *Journal of Global Research in Computer Science*, IISN-2229-371X, Volume 3, No. 12, December 2012.

[76] Minati Mishra, Priyadarshani Mishra and M.C.Adhikary, "Digital Image Data Hiding Technique : A comparision Study", ISSN-0974-715X , ANSVESA, 7(2), 105-115, 2012.

[77] R. Poornima, R J Iswarya, "An Overview of Digital Image Steganography", *International Journal of Computer Science & Engineering Survey (LJCSES)*,Vol 4. No.1.February 2013.

[78] Ankita Sancheti, "Pixel Value differing image steganography using secret key", *International Journal of Innovative Technology and Exploring Engineering (IJITEE)* ISSN: 2278-3075, Volume-2, Issue-1, December 2012.

[79] Joshua_C_Clark, "Digital Steganography : A Symmetric Key Algorithm".

[80] Jiri Fridrich, "A new stegangraphic method for pallete-Based images", Center for Intelligent Systems, SUNY Binghamton, Binghamton, NY 13902-6000.

[81] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital image steganography: Survey and analysis of current methods", School of Computing and Intelligent Systems, Faculty of Computing and Engineering, University of Ulster at Magee, Londonderry, BT48 7JL, Northern Ireland, UK.

[82] Andreas Westfeld, "Detecting Low Embedding Rates", Institute for System Architecture, Technische Universit¨at Dresden, 01062 Dresden, Germany, F.A.P. Petitcolas (Ed.): IH 2002, LNCS 2578, pp. 324–339, 2003,c_ Springer-Verlag Berlin Heidelberg 2003.

[83] Shikha Choksi, "Comparitive Study on Authentication Schemes for Cloud Computing", 2014 IJEDR 1402238, 2785| Volume 2, Issue 2 | ISSN: 2321-9939.

[84] H S Manjunatha Reddy, K B Raja, "HIGH CAPACITY AND SECURITY STEGANOGRAPHY USING DISCRETE WAVELET TRANSFORM", Dept. of Electronics and Communication Global Academy of Technology, *International Journal of Computer Science and Security (IJCSS)*, Volume (3): Issue (6).

[85] Hsien-Chu Wu,Na-I Wu,Chwei-Shyong Tsai,Min-Shiang Hwang," An Image Steganographic Scheme Based on Pixel-Value Differencing and LSB Replacement Methods", Department of Management Information System Min-Shiang Hwang National Chung Hsing University, November 7, 2004.

[86] Nagham Hamid, Abid Yahya, R. Badlishah Ahmad, Osamah M. Al-Qershi, "Image Steganography Techniques: An Overview", *International Journal of Computer Science and Security (IJCSS)*, Volume (6) : Issue (3) : 2012.

[87] Jarno Mielikainen, Member, IEEE, "LSB Matching Revisited", *IEEE SIGNAL PROCESSING LETTERS*, VOL. 13, NO. 5, MAY 2006.

[88] Farhan Khan, Adnan Abdul-Aziz Gutub, "Message Concealment Techniques using Image based Steganography".

[89] Debiprasad Bandyopadhyay, Koushik Dasgupta, J.K. Mandal, Paramartha Dutta, "A Novel Secure Image Steganography Method Based On Chaos Theory In Spatia Domain", *International Journal of Security, Privacy and Trust Management (IJPTM)* Vol 3, No 1, February 2014.

[90] Saurabh V. Joshi, Ajinkya Bokil, Nikhil A. Jain, Deepali Koshti, "Image Steganography Combination of Spatial and Frequency Domain", *International Journal of Computer Applications (0975-8887)*, Volume 53-No. 5, September 2012.

[91] J.K. Mandal, "A Frequency Domain Steganography using Z Transform (FDSZT)".

[92] Nedal M. S. Kafri, Hani Y. Suleiman, "Bit-4 Frequency Domain-DCT Steganography Technique".

[93] Dr. Mahesh Kumar, Munesh Yadav, "Image Steganography Using Frequency Domain", *International Journal of Scientific & Technology Research*, Volume 3, Issue 9, September 2014, ISSN 2277-8616.

[94] Palak Mahajan, "Steganography : A Data Hiding Technique", *International Journal of Advanced research in computer Science and Software Engineering*, Volume 4, Issue 11, November 2014, ISSN: 2277 128X.

[95] N. Lavanya,V. Manjula, N.V. Krishna Rao, "Robust and Secure Data Hiding in Image Using Biometric Technique", *International Journal of Computer Science and Information Technology*, Vol. 3(5), 2012, 5133-5136, ISSN: 0975-9646.

[96] Saeede Goodini, Mahdi Jafari Shafbazzadeh, "New Method of DWT-based Image Steganograph by using Fuzzy Logic", Current Trends in Technology and Science, ISSN : 2279-0535.

[97] M. Sifuzzaman , M.R. Islam and M.Z. Ali , " Application of Wavelet Transform and its Advantages Compared to Fourier Transform", *Journal of Physical Sciences*, Vol. 13, 2009, 121-134, ISSN: 0972-8791.

[98] Richa Gupta, Sunny Gupta, Anuradha Singhal, "Importance and Techniques of Information Hiding", *International Journal of Computer Trends and Technology (IJCTT)*, Volume 9, Number 5, Mar 2014, ISSN: 2231-2803.

[99] Richa Gupta, "Information Hiding and Attacks: Review", *International Journal of Computer Trends and Technology (IJCTT)*, Volume 10, Number 1, Apr 2014, ISSN: 2231-2803.

[100] Stefan Katzenbeisser Fabien A. P. Petitcolas, "Information Hiding Techniques for Steganography and Digital Watermarking", ARTECH HOUSE, Computer Security Series.

[101] Arvind Kumar, Km. Pooja, "Steganography- A Data Hiding Technique", *International Journal of Computer Applications (0975 – 8887)* Volume 9– No.7, November 2010.

[102] Abbas Cheddad, Joan Condell, Kevin Curran, Paul Mc Kevitt, "Digital image steganography : Survey and analysis of current methods", Signal Processing 90 (2010) 727-752.

[103] Neil F. Johnson, Stefan C. Katzenbeisser,"A Survey of Steganographic Techniques", Information hiding techniques for steganography and digital watermarking.

[104] Alisha Arora, Mrs. Nirvair Neeru, Mrs. Taqdir, "Image Steganography Techniques: An Overview", *International Journal For Technological Research In Engineering*, Volume 1, Issue 9, May- 2014, ISSN (Online): 2347 – 4718.

[105] Deepa S, Umarani R, "A Study on Digital Image Steganography", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 3, Issue 1, January 2013, pp.54-57, ISSN:2277 128X.

[106] Mr. Falesh M. Shelke, Miss. Ashwini A. Donger, Mr. Pravin D. Soni, "Comparison of different techniques for Steganography in images", *International Journal of Application or Innovation in Engineering & Management (IJAIEM)*, Volume 3, Issue 2, February 2014, ISSN 2319-4847.

[107] Mukesh Garg, A.P. Gurudev Jangra, "An Overview of Different Type of Data Hiding Scheme in Image using Steganographic Techniques", *International Journal of Advanced Research in Computer Science and Software Engineering*, Volume 4, Issue 1, January 2014, ISSN:2277 128X.

[108] Navneet Kaur, Sunny Behal, "A Survey on various types of Steganography and Analysis of Hiding Techniques", *International Journal of Engineering Trends and Technology (IJETT),* Volume 11 Number 8 – May 2014.
[109] Shamim Ahmed Laskar, Kattamanchi Hemachandran, "High Capcity data hiding using LSB Steganography and Encryption", *International Journal of Database Management Systems (IJDMS),* Vol.4, No.6, December 2012.
[110] T. Morkel, J.H.P. Eloff, M.S. Oliver, "An Overview of Image Steganogrphy", Information and Computer Security Architecture (ICSA) Research Group.
[111] Taras Holotyak, Jessica Fridrich, David Soukal, "Stochastic Approach to Secret Message Length Estimation in +_ k Embedding Steganography".
[112] Vikas Verma, Rishma Chawla, "Image Block-based Steganography using Varying Size Approach", *International Journal of Computer Applications (0975-8887),* Volume 97-No. 13, July 2014.
[113] Ming Li, Michel Kulhandjian, Dimitris A. Pados, Stella N. Batalama, Michael J. Medley, "PASSIVE SPREAD-SPECTRUM STEGANALYSIS".
[114] Basavaprasad B, Ravi M, "A STUDY ON THE IMPORTANCE OF IMAGE PROCESSING AND ITS APLLICATIONS", IJRET: *International Journal of Research in Engineering and Technology,* eISSN: 2319-1163 | pISSN: 2321-7308.
[115] A.Anuradha, Dr. Hardik B. Pandit, "A Review on information hiding techniques, A Comparative Analysis", IJRET: *International Journal of Research in Engineering and Technology,* eISSN : 2319-1163| pISSN: 2321-7308.

WEB REFERENCES

[116] http://shodhganga.inflibnet.ac.in (20/05/2016)
[117] researchgate.net (04/05/2016)
[118] Fullform.net (25/05/2016)
[119] http://ieeexplore.ieee.org (13/06/2016)
[120] www.sciencedirect.com (15/06/2016)
[121] stackoverflow.com (24/07/2016)
[122] http://datagenetics (30/07/2016)

