ENHANCED IMAGE COMPRESSION MECHANISM TO INCREASE EFFICIENCY OF BIOMETRICS

[1]**Muskaan,** [2]**Deepika**

1Research Scholar, Department of CSE, IIET, Kinana

2A.P, Department of CSE, IIET, Kinana

ABSTRACT: - Biometrics has been considered as machinery. It categorizes the different kind of human being. It has been done to measure and analyze one or more unique behavior. The uniquely categorization may be made by measuring the physical traits. Proposed mechanism has been determined best as compare to present biometrics application. The Image compression is a sort of data compression. It is utilized with digital graphics, in order to reduce the cost for storage. The present work is providing the review of several image compression mechanisms. The discussed techniques are Loosy Image Compression Methods and Lossless Image Compression Methods. In this paper the explanation of discussion is made on an algorithm based on compression of the graphics. This algorithm is capable to reduce the loss in quality of the graphics content in biometric system. This paper is providing the explanation of PSNR calculation at the time of image processing. PSNR calculation is capable to enlarge the efficiency of biometric. The proposed system is different, making comparison to existing biometrics application. The proposed work would introduce the security at registration level and at transaction time. It can be considered highly appropriate for image transmission at the time of networking.

KEYWORD: - Biometrics, Image processing, PSNR, Image compression

[1] INTRODUCTION

The Biometric systems are involved in any system to use the application of biometric system. The biometric applications enable to identify the automatically, verification or authentication of any natural person. In principle, biometric systems are used to process the personal data. By privacy specialist it has been used to justify the high level of security. For strict identification, the biometrics systems are used.

Most of biometric application assists to basic functional components. These components may be:

- The biometric storage entity with biometric samples of data of enrolled individuals. It has been linked or integrated in a database within individuality data of corresponding individuals.

- The Biometric sensor device and pre-processing capacities have been used to capture biometric sample data from an individual as input data.

- Comparison procedures evaluate the similarity between reference template and captured data sample. Then it calculates a matching score.

Fig 1 Biometric Image

[2] IMAGE COMPRESSION

The Image compression has determined one sort of data compression. It has been applied with digital images. It is capable to decrease the storage or transmission. Algorithms may provide the advantage of visual perception and statistical properties of graphic information. It offers the superior results compared with generic compression methods.
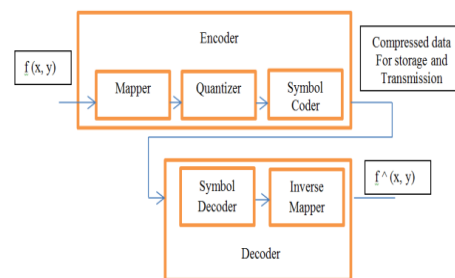

Fig 2 Image compression [1]

Image compression minimizes the size in bytes of a graphics file. As well as it retains the quality of image to a not acceptable stage. To reduce the size of file allows the extra graphics in provided disk or may be memory space. It also decrease the time demanded for graphics to be sent over Internet or downloaded from Web pages.

[3] REVIEW OF LITERATURE

In this research we would use image processing toolbox in MATLAB in order to compress image without losing quality of image. In order to perform this we have to study researches related to image processing.

In 2012, M. Mozammel Hoque Chowdhury et al[1] wrote on image compression with the use of discrete wavelet transform. It is known that the Image compression has been considered a key technology. It has been applied in dealing and storage of digital graphics. The cause is its dealing with a huge size of images.

In 2013, Akshay Kekre [2] did research on image compression with the use of wavelet transform and differential pulse code modulation technique. Image compression has been applied in order to reduce the unimportance and redundancy of the picture data. It enables the user to save or transmit data in an able form. The comparison is made by selecting several amalgamation of band and measuring the compression ratio and PSNR.

In 2013, Miss. S.S. Tamboli1, et al [3] explained the image compression applying HAAR wavelet transform. They have reported is aimed at developing computationally efficient and effective algorithm. These are used for lossy image compression applying wavelet techniques. Therefore this proposed algorithm has been developed in order to compress image so fatly. The Promising outputs got the concerning reconstructed quality of picture and conservation of significant image details. On other side, a high compression rate is there.

In 2014, Dr. Vineet Richariya et al [4] image compression technique. The research has been done applying several wavelet functions. With the progress of Digital image processing methods, several applications there are. One of applications is an image compression. The paper has assigned a comparative review has been made with the use of several wavelet function. These may be Hear, dB4 &

dB6 for compression and reconstruction of graphics applying MATLAB. It also considers the PSNR, Entropy, Energy & compression ratio of graphics.

In 2015, Malwinder Kaur [5] proposed a literature review on lossless image compression. To decrease the redundancy of the image data is the main objective of image compression. It allows the user to enlarge the storage capacity and proficient transmission. They have proposed the chief approach of image compression. Vital parts have been discussed in this paper. The researcher has presented an overview of multiple traditional coding standards lossless image compression mechanism.

In 2016,Er. Kiran Bala, et al [6] did research on advance digital image compression. They have used the fast wavelet transforms comparative analysis with DWT. The research has offered the FWT based image compression. It is used in order to get desired results of proposed work. Image Compression has been performed in MATLAB software with the use of wavelet toolbox.

In 2017, Anurag, et al [7] stated the JPEG Compression. They have used the MATLAB to fulfill their objective. Camera sensor are able to create big size of data. to store this data is not a simple task. As a result the efficiency is very poor. Mobile or bandwidth- limited a system formulates the especially cumbersome. Here the object is a conservative bandwidth cost, for example the World Wide Web. The MATLAB code and technology used to achieve a fast way. It offers the way to search the JPEG algorithm.

In 2010, E. P. Kukula, et al [8] wrote on the Human – Biometric-Sensor Interaction Evaluation Method. The paper has stated the Biometric Performance and Usability Measurements. They have described the human–biometric-sensor interaction. The sort form is HBSI evaluation method. By this way the ergonomics, usability, and sample quality criteria are applied as explanatory variables. It is used for the overall biometric system efficiency. The results in this paper has revealed on fact. The traditional bio-metric evaluations concentrates on system-level metrics. These are not pro- viding efficient reporting details related the user dealing with the mechanics. These three metrics may be false interaction, failure to detect and concealed interaction.

In 2010, C. Rathgeb et al [9] did research on iris-biometric hash generation. It has been used for biometric database indexing. In order to perform the categorization on big-size, the biometric databases require an exhaustive linear search. The biometric data does not have any natural sorting order and indexing databases. To decrease the response time of the system indicates a huge size challenge. They have proposed a biometric hash generation method. It has been done to fulfill the aim of biometric database indexing. It has been used to iris biometrics. The final results has shown the presented concept of highly accelerates biometric clarification.

In 2014 S. C. Eastwood, et al [10] discussed the Biometric Intelligence in Authentication Machines. The research is related to the talking Faces to talking Robots. The focus of this paper is on intelligent human-machine interfacing of behavior biometrics. It has a vital role in future times of A-machines. Numerous pilot projects use the talking face method. They have suggested the further process to A-machines based on talking robot technology. Interviewing the traveler, a humanoid robot differentiates the faces and expressions. It varies the e-passports and the traveler. It may be connect with a watch list. It generates the cognitive questions and evaluation answers,

In 2014, J. Galbally et al [11] discussed the image quality assessment for fake biometric detection. They also discussed the application to iris, fingerprint, and face recognition. It is essential to make sure the real attendance of a real legitimate trait on the contrary to a fake self-made the synthetic or reconstructed sample. It is very vital issue in biometric verification. It demands the improvement of innovative and efficient security measures. In this paper, we present a novel software-based fake detection method that can be used in multiple biometric systems to detect different types of fraudulent access attempts. There is an objective of the presented system. To protect the biometric recognition designs the biometrics systems are used. It has been done by the liveness assessment in a fast, user-friendly, and non-intrusive manner. It is feasible by the use of image quality assessment. Proposed concept proposed a very low degree of complexity. It makes it suitable for real-time applications, with the use of 25 general image quality features extracted

from one image. It has been done to distinguish the legitimate as well as impostor samples. It indicates the proposed method is highly competitive compared with other state-of-the-art approaches. The evaluation of the general image quality of real biometric samples reveals highly valuable data. It may be sufficiently applied to distinguish them from fake attributes.

In 2015, I. Sponsored, et al [12] provided a paper to enhance the Security for Multimodal Biometric using Hyper Image Encryption Algorithm. The consumption of huge-size biometric application is used in commercial and government sector. These are used to enlarge the attentiveness of public of this methodology. This dramatic growth in biometric system has clearly point out the challenges connected to design and integrate such systems. 'Multimodal biometrics' is development to great importance wherein the information from three different biometric sources namely finger print, retina, finger vein is used for authentication system. Unlike not biometric systems, these are sensitive to noise and make spoofing difficult for hackers. These are used as a deployment of multimodal biometric. The aim of the project is to dynamically make sure the efficiency of the systems. It has been done to offer an enhanced stage of protection. It has been done to combine Finger vein, Retina and Fingerprint with Hyper Image Encryption Algorithm.

In 2015, R. Tolosana, et al [13] stated the preprocessing and feature selection for improved sensor interoperability in Online Biometric Signature Verification. In this paper, we focus on interoperability device compensation for online signature verification since this biometric trait is gaining a significant interest in banking and commercial sector in the last years. The presented concept has dependence on two basic level stages. First level is a preprocessing stage. Here the data is achieved from several devices. The data is processed to normalize the signals in same levels. The other level is related to the feature selection having in account the device interoperability situation. It has been done to choose features rousted in these situation.

In 2016, M. Bellaaj et al [14] wrote on possibilistic modeling palmprint and fingerprint. It is related to the multimodal biometric recognition system. One

tool has been used to deal with imperfections and redundancy of dat. the possibilistic modeling has been considered an efficiency way. The work has proposed a robust multimodal biometric recognition system integrating fingerprint and Palmprint. It is related to the possibilistic modeling concept. The offered concept is based on possibility theory concepts. It has been used to model the biometric features.

In 2017, J. Dong, X. Meng, et al [15] did research on template protection based on DNA coding for multimodal biometric recognition. The final conclusion shows that their experiment reveals on thing. Proposed multimodal biometric template protection scheme don'ts influence the recognition efficiency. It also makes sure the security of multimodal biometric template.

In 2017, R. Devi et al [16] provided a review on biometric and multi-modal biometric system. The paper also involves the modules, applications, techniques and challenges. To identify a person has been considered a vital job in our daily life. Conventional way involves the password, ID cards, etc. on the other hand these identities can normally be misused. It may be lost or shared. To conquer the above challenges of the conventional ways, the biometric system has been launched. Biometric system has a vital role to provide the high-security applications. These may be border control, immigration etc. the paper offers the detailed review of several modules, applications. It also explained the methods and challenges of the multimodal biometric system.

[4] OBJECTIVE

The theme of this research is to secure biometrics system in ecommerce application & provide following features to system.

1. Encode user using biometric sample data at time of storing in database.
2. Decode data using biometric when user login to allow him to access his own account.
3. Restrict user to make transaction using biometric.
4. Making digital wallet available to him if we are correctly logged in as well as he has inserted correct biometric sample.

5. More over at time of transaction from digital wallet one time password would be generated so that it could be access by user.

[5] PROPOSED WORK

1. Securing user data at time of storing in database.
   When user submits data from sign up form then information is encrypted using cryptographic algorithm and using biometric sample as key so that hacker could not access general information of user.

2. Permits user to access data. When user login it permits him to access his own account.
   Information of user is stored in hidden form so user should be able to access information at time of login. As soon as user successfully logs in he could do transaction to buy product.
3. A biometric security is applied to restrict user to make transaction. Once user enters valid biometric sample he would be eligible to perform transactions.
4. Digital wallet allows user to buy product from own balance. In proposed work we are making digital wallet available to him if we is correctly logged in as well as he has inserted correct biometric sample.
5. At time of transaction from digital wallet one time password would be generated so that it could be access by user. This OTP could be send to him using email or SMS.

[6] CONCLUSION

The proposed system is far better than traditional biometrics application. Here the security at registration level has been discussed as well as at transaction time. The research has studied effective means by which content of image could be automatically structured, indexed & retrieved. This research has studied the various image compression techniques are loosy Image Compression Methods & Lossless Image Compression Methods. In proposed work an algorithm based on Huffman Coding has been design to

compress image with minimum loss in quality of image. It is most suitable for image transmission during networking.

[7] SCOPE OF RESEARCH

The proposed system would be far better than traditional biometrics application. It would introduce the security at registration level as well as at transaction time. It would the studied effective means by which content of image could be automatically structured, indexed & retrieved. In proposed work an algorithm based on Huffman Coding has been design to compress image with minimum loss in quality of image. It is most suitable for image transmission during networking. This research would be study of various image compression techniques are loosy Image Compression Methods & Lossless Image Compression Methods.

REFERENCES

[1] M. Mozammel Hoque Chowdhury and Amina Khatun(2012) "Image Compression Using Discrete Wavelet Transform" International Journal of Computer Science Issues, Vol. 9, Issue 4, No 1, July 2012

[2] Akshay Kekre(2013) "Image Compression Using Wavelet Transform And Differential Pulse Code Modulation Technique" International Journal of Engineering Research & Technology (IJERT) Vol. 2 Issue 7, July – 2013

[3] Miss. S.S. Tamboli1, Dr. V. R. Udupi (2013), "Image compression using haar Wavelet transform", International Journal of Advanced Research in Computer & Communication Engineering Vol. 2, Issue 8, August 2013

[4] Dr. Vineet Richariya Mrs. Shweta Shrivastava Naman Agrawal (2014), "Image Compression Technique Using Different Wavelet Function", International Journal of Research in Computer & Communication Technology, Vol 3, Issue 5, May-2014

[5] MalwinderKaur(2015)A Literature Survey On Lossless Image Compression

[6] Er. Kiran Bala, Varinderjit Kaur (2016), "Advance digital image compression using fast wavelet transforms comparative analysis with DWT", International Journal of Engineering Sciences & Research Technology Bala et al., 5(7): July, 2016

[7] Anurag, Sonia Rani(2017) "JPEG Compression Using MATLAB" 2017 IJEDR | Volume 5, Issue 2

[8] E. P. Kukula, M. J. Sutton, and S. J. Elliott, "The Human – Biometric-Sensor Interaction Evaluation Method : Biometric Performance and Usability Measurements," pp. 1–8, 2010.

[9] C. Rathgeb and A. Uhl, "Iris-Biometric Hash Generation for Biometric Database Indexing," 2010.

[10] S. C. Eastwood, V. P. Shmerko, S. N. Yanushkevich, and M. Drahansky, "Biometric Intelligence in Authentication Machines : From Talking Faces to Talking Robots," 2014.

[11] J. Galbally, S. Marcel, and J. Fierrez, "Image Quality Assessment for Fake Biometric Detection : Application to Iris , Fingerprint , and Face Recognition," vol. 23, no. 2, pp. 710–724, 2014.

[12] I. Sponsored, S. International, and C. On, "Enhancing Security for Multimodal Biometric using Hyper Image Encryption Algorithm,," pp. 943–947, 2015.

[13] R. Tolosana, R. Vera-rodriguez, J. Ortega-garcia, S. Member, and J. Fierrez, "Preprocessing and Feature Selection for Improved Sensor Interoperability in Online Biometric Signature Verification," vol. 3, 2015.

[14] M. Bellaaj, R. Boukhris, A. Damak, and D. Sellami, "Possibilistic Modeling Palmprint and Fingerprint based Multimodal Biometric Recognition System," pp. 1–8, 2016.

[15] J. Dong, X. Meng, and M. Chen, "Template Protection Based on DNA Coding For multimodal biometric recognition," no. Icsai, pp. 1738–1742, 2017.

[16] R. Devi and A. Prof, "A Study on Biometric and Multi-modal biometric system modules , Applications , Techniques and Challenges," no. March, pp. 3–4, 2017.