VOL. 10, NO. 8, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

MUTUAL AUTHENTICATION USING IMAGE PROCESSING AND VISUAL CRYPTOGRAPHY PROTOCOL FOR PATIENT DATABASE

B. Padmavathi, Vishrut Sharma, Sungkrityayan Khan and Adithya Krishnareddy
Department of Computer Science and Engineering, SRM University, Chennai, India
E-Mail: hod.cse@vdp.srmuniv.ac.in

ABSTRACT

Online Patient database is a particular type of service rendered by a chain of intercommunicated hospitals. Medical practitioners and clients are able to access their records or look into status of their diagnosis from any of the other or branch hospitals. The principle concern in online patient database is the authenticity of both the doctor and the client. Due to ineluctable intruding of the database on the Internet, it is very hard to rely on any kind of data on the Internet. The propounded approach of ours, based on Image processing technique and Visual Cryptography, the authentication problem is resolved. This particular paper proffers a technique of processing the Endoscopic Ulcer images based on Grow-cut and then divides it into Secret shares based on Random Grid Visual cryptographic Techniques. The total number of shares to be created depends on the strategy selected by the medical practitioner. If two shares are prepared, one of the shares is reposited in the Global Hospital Server, and the other is retained by the client. The client has to produce his/her secret share during the consultation. Client's share is then stacked with the Hospital Server share to obtain the original Endoscopic image. This method of correlation aids in concluding the decision based on espousal or denial of the output and hence confirms the client.

Keywords: random grid based visual cryptography, endoscopic ulcers, ROI, foreground extraction, image editing, interactive image segmentation, global hospital server, secret shares.

1. INTRODUCTION

With the advancement of communication techniques and information relating to digital media (such as video, audio, image and text), the arbitrary exploitation of such data, is also proliferating. Certain domains, however require strict control over the Authenticity, duplication, modification and distribution of these datas. Medical images and their attributed details are an example of one such field [1]. To safeguard data and authorize only permissible changes, strict security has to be ensured. The convenient exchange of patient data, between treatment centers and hospitals, is a common practice. However this practice also allows for changes to occur, when exchanging data through the internet. The internet does not prevent changes to occur in medical images, this could lead to crucial information getting disoriented or corrupted. Medical images lack delineation of anatomical structures, and regions of interest because they are constantly marred with distractions due to noise (random or white noise) and ambiguity over boundary and region information. The use of robust techniques like median filtering and grow-cut method of image segmentation , have been found to be efficacious in mitigating user efforts for precise image extraction and enhancing the quality of the image. Encryption techniques like Random Grid based Visual cryptography hence play a crucial role, in safeguarding images, ascertaining their security and ensuring authenticity.

Statistical aberrations in images are minimized by using noise filters, which apply essentially 3 methods. They are namely:- 1)Adaptive filtering, 2) Median filtering and lastly, 3) Sigma Filtering. In our propounded approach we have implemented median filtering, where pixel intensity is set to a median intensity of adjoining pixels, hence eliminating intensity spikes. The paper also demonstrates the use of "grow cut " method for image segmentation, which is an interactive method, and is known to mitigate the issues in automatic image segmentation. It extracts a distinct region in an image, from its background, with the least amount of human interaction possible. The advantage of deploying this method onto medical images, is that it provides locally as well as globally the most optimal solution of the specimen for image segmentation.

Although Visual Cryptographic techniques are usually applied for secure transmission of secret images, we have extended its ability to provide Mutual Authentication for Medical Images.

Numerous existing methods for image processing and visual cryptographic protocols have been discussed in Section 2. We have discussed our propounded based on image processing and visual cryptography in Section 3. The results have been given in Section 4. In the last section, we have given the conclusion and future works.

2. EXISTING METHODOLOGIES

A brief survey of image segmentation techniques and the applications of visual cryptographic schemes in various fields have been discussed in this section. Image segmentation has found numerous applications in the field of image processing. It has been widely applied for the analysis of medical images and for photo editing. Numerous fully automated segmentation techniques are available in the market, which are perpetually ameliorated. On the contrary, image analysis techniques that are fully automatised in nature, which can be employed without any external control with ensured results in general case.

Henceforth semi-automatic segmentation techniques that have the ability of resolving intensely hard segmentation jobs by the application of a small effort on

behalf of the user are seemingly gaining popularity [10]. Recently, numerous powerful techniques have been propounded for interactive image segmentation based on grab-cut, graph cuts [2], [4] and random walker [3], [12]. They have significantly outperformed the older methods both in terms of resulting segmentation quality as well as required user effort.

Boykov and Jolly [2], [7] implemented graph cut technique for the task of segmenting the organ images. The technique considers the entire image as a graph and the pixels of the image are taken as a graph node. This technique is efficacious for N-dimensional images [12]. Rother *et al*. [8] has implemented the grab-cut technique by keeping on iterating graph-cut for intermediate steps while doing interactive foreground extraction. After the iterations come to a halt, the results of segmentation can be fine-tuned by mentioning additional seeds, alike the original graph-cut.

Even, the advancement of communication techniques and information relating to digital media (such as video, audio, image and text), leads to the arbitrary exploitation of such data. So there is an neccessity for exercising strict control over the duplication , modification and distribution of these datas. Steganography, in today's modernization of the electronic era, is the ability of concealing the very presence of the message in extra bits of any unremarkable media [5]. Cryptography does not conceal the noesis about the information being present in the cover media but the data is encrypted as the cipher-text and disputes decoding it without authorization; i.e., cryptography concentrate on challenging the decoding process.

On the other hand, watermarking is different from visual cryptography in the sense that it aims in protecting the cover media from any alterations with no true stress on secrecy [6]. Watermarking technique is defined as the process of protecting intellectual image property in digital form. This destroys the image quality to a larger extent. On the other hand, Visual Cryptography is highly focusing on robustness and ameliorated authentication. Visual cryptography enables in concealing the visual data (text, pictures, etc.) into two secret shares, such that when these shares are decrypted together, retrieves the hidden visual information(i.e., pictures, texts etc.).

Moni Naor and Adi Shamir [9], developed visual cryptography in 1994, as a method of encrypting visual data, by a covert sharing scheme. It allows veiled distribution of visual data, without performing cryptographic computations or compromising on the security of data. Essentially, the image to be encrypted is fragmented into n shares. A minimum of 2 transparent shares are used in cryptography. One split only holds irregular pixels, and the other subsumes the secret information. Having any one of the shares is futile, as the information held in a single share is abstruse and recondite. Upon merging of both the shares, the concealed data can be fetched successfully. This method is applicable to shadow images with n shares, which on stacking reveals the concealed information (data).

Borchert [11] proposed a segment-based visual cryptography applicable only to encrypt the bank related messages containing numbers, symbols etc. Wei-Qi Yan *et al*., [13] suggested a visual cryptography scheme applicable solely for printed texts or images. Monoth *et al*. [14] suggested a recursive visual cryptography scheme for encoding shares into sub shares recursively. Kim *et al*. [15], has also proposed a similar recursive scheme pixel dithering.

Unfortunately, visual cryptography protocol has been found to be affected by the "cheating problem" [16], [17] where the decrypted concealed image gets modified due to malicious insiders namely "cheaters." Specifically in these scenarios, participants whoever are assumed to be holding shares are generally considered to be honest, i.e., fake shares won't be exhibited by them during the phase of visual cryptographic decryption. Hence, the image procured on decrypting the secret shares are considered to be the real concealed image. But this isn't the original scenario always. So, a cheating prevention technique namely, Random Grid scheme is used.

Random Grid algorithm avoids pixel expansion while creating shares [18], [19]. It provides a unique feature to each participant for verifying other participants share. Hence cheaters are eliminated. Shares of participants are not alike in nature, and are highly confidential. The concealed images contrast is lessened to a greater extent during the decryption of the visually cryptographic shares. A mutual authentication applicable to any visual cryptographic scheme is rendered by this algorithm. In this paper, we have propounded a visual cryptographic scheme based on Non-Expansible Random Grid algorithm and Three Party Mutual Authentication.

3. PROPOSED METHODOLOGY

A. Image acquisition

The procured endoscopic ulcer images from the process of endoscopy, are exhibited in 2D matrix, where the image pixels are considered as the elements. Such type of matrices depends on field of view and size of the matrix. The endoscopic images are stored using MATLAB and are displayed as gray scale images having a dimension of 256*256. The gray scale is nothing but the interval [Lmin, Lmax]. The ubiquitous practice is to transpose this interval, with regards to the interval [0, L-1], where L=0 is considered as black and l=L-1 is considered to be as the white on the gray scale. Any intermediate values within this range are shades of gray from black to white. These endoscopic images procured from endoscopy are stored in JPEG formats.

B. Image restoration

In image enhancing, the principle concern of the restoration techniques is to ameliorate an image based on some beforehand knowledge. Image retrieval or re-modeling aids in restoring those images, whose quality has been reduced due to the existence of noises. In digital images, noises arises during image acquisition (digitization) and/or transmission. In this image restoration

phase, minute details are ameliorated and noise is filtered. Generally used noise filtering techniques like adaptive filtering, linear filtering etc., are applied, for the procurement of feasible results.

In this particular paper, we have used the median filtering approach for the removal of impulse, or salt-and-pepper noise. These noises are due to the random bit error in a communication channel. Median filtering is an efficacious way of smoothening the impulse noise as well as it effectively preserves the edges. Thus reducing the obscuring impression of the image and the possible twisted results of the intervening system. Eventually grow-cut segmentation will also be implemented. This ameliorated image aids in edge determination and ameliorates the overall image quality.

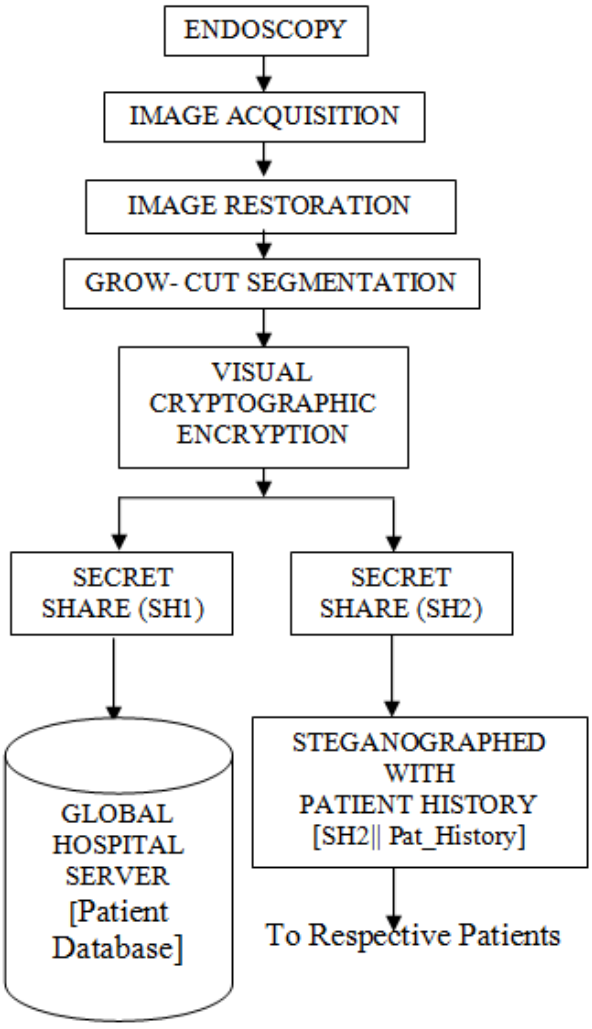

Figure-1. Proposed architecture system.

C. Grow-cut segmentation

The endoscopic ulcer image segmentation is done by the implementation of a cellular automation technique known as the grow-cut method. In this methodology, the segmentation is initiated by the selection of seed points. The segmentation process operates by implementing a set of user inputs in the form of "object" and "background" brushes for foreground and background. Eventually, the seed pixels and the label strengths are fixed by each paint stroke of a pre-defined set of brush. The incomplete user labelling at the beginning is often ample to permit the entire segmentation process to be completed automatically (not compulsorily). When all the pixels in the region of interest are labeled, the algorithm tends to meet, and no labels can be changed by any pixels any further.

The user can monitor the progress and interact at the right time as well as guide the labeling process, if at all there is a necessity, when the cell labels are being calculated. Adding of segmentation constraints in the form of user editing takes place. Each new paint strokes affect the underlying pixel states and hence the automaton evolution is affected as a result. The above proposed method allows acquiring or extracting the region of interest from complex backgrounds using the simple strokes of a paint brush done by the help of a mouse.

D. Random grid visual cryptographic encryption

An efficacious system is designed in our propounded project to render mutual authentication and secured medical data transfer in an insured way. To realise this concept in reality, we have implemented Random Grid visual cryptography as the principle concept. A Global Hospital Server is designed to store the registered patient's history and their Medical Images in a concealed manner. This system allows multiple hospitals to get registered to the Global Hospital Server (GHS). Hence, automatically the doctors from those hospitals are registered with the server. All the patients who get treated there also become registered. All the patient reports in the form of Scan, X-Ray, MRI are saved in the GHS in the form of medical images. It is mandatory for the images to be half-toned, and if they aren't, they are converted to the needed form by implementing the halftone generation algorithm. These images should be of n*n pixels. All these images are encrypted into two Secret Shares by applying Non Expansible Random Grid Visual Cryptographic Algorithm. One of the shares SH1 is saved in the GHSDB along with Patient ID. The generation of the quotidian share is haphazard and the generation of the remaining shares occurs due to the comparison between the images taken as input and the generated quotidian share. Whilst the patient registration, all the shares relevant to the patients will be saved by the server as SH2. This patient's secret share SH2 is steganographed with his treatment details, and is sent to the patient. This is clearly as shown in Figure-1

Whenever, the patient wishes to go for a medical review, at any time and place he can carry this electronic data and can meet any available doctor. The doctor desteganographs the medical history from the electronic data and extracts the SH2 alone. The doctor simply sends this data along with his/her identity to the GHS. The server searches for the corresponding SH1 for the patient, retrieves the corresponding SH1.

The Server applies visual cryptographic decryption and verifies the obtained medical image with the original endoscopic image of the Patient. If they match and the patient is authenticated, his medical image is sent to the doctor. The doctors can further diagnose the current condition of the patient and can treat him accordingly. He updates the patient history and submits it along with the medical image. The GHS once again steganographs the updated patient details into his SH2. Thus all the parties involved are mutually authenticated by this protocol.

The Multi-party Mutual Authentication has been implemented in three modules by the propounded approaches which are as follows:

I) Pseudo code of random grid method

Visual cryptography enables to conceal the visual data (text, pictures, etc.) into two secret shares, such that when these shares are piled together, retrieves the concealed visual data (i.e., pictures, text etc.). The decrypted visual information is comparatively darker than the backgrounds.

In this share creation phase, Half-tone images of dimensions 512*512 pixels are taken into consideration as inputs. If the images, provided as input to the system, are not half-toned, rather they are found to be coloured having various sizes, then these images are transformed to the half-tone images, having the above mentioned dimension.
The Random Grid Algorithm proposed by Wang *et al*., [18], has been implemented for the share creation. If two images are provided as inputs to the server, three shares would be generated, which are named as Quotidian share or Share 1 (SH1) and Share 2 (SH2). The secret share's empty upper grids namely SH1U, SH2U, and the secret share's empty lower grids namely, SH1L and SH2L are generated by the algorithm and eventually 0's and 1's fills those generated grids, by the comparison of each pixel with that of the input concealed images. In this share creation process, pixels are not expanded which results in maintaining the share size, which is always the same when compared with the input images. The following Random Grid Algorithm by Wang *et al* of [18] produces the shares.

Algorithm

Input: Original endoscopic medical image namely, Img1, and it is a halftone image and the size of the input image is 512*512 pixels.
Output: Shares SH1, SH2

Step. 1 The pixel values of SH1U and SH1L are assigned randomly.

Step. 2 The pixel value of SH2U is assigned.
if ImgU[x][y] = white then SH2U[x][y]= SH1U[x][y].
else
SH2U[x][y]=complement of SH1[x][y].
end if

Step 3. The pixel value of SH2L is assigned.
If ImgL[x][y] = white then SH2L[x][y]= SH1L[x][y].
else,
SH2L[x][y]=complement of SH1[x][y].
end if

The generated secret shares and the resultant images of stacking are shown in the Results part.

II) Secret image generation by random grid method

Bit by bit comparison of the generated shares and eventually the application of Bitwise XOR operation aids in the procurement of the secret images. The upper and the lower grids conforming in every respect with the shares SH1 and SH2 are stacked together for the Secret Medical image generation. In, the stacking operations, mainly the pixel of two shares are compared row and column wise. In the first secret image, if the pixels belonging to each of the two shares are having the same color, it results in the generation of a white pixel otherwise, it results in the generation of a black pixel, in case the pixels comprises of different color. This particular logic of pixel generation resembles bitwise XOR operation. Hence the secret medical image of a patient is exposed by the stacking of shares SH1 and SH2, one upon the other.

The secret shares that are generated and the resultant patient medical images are shown in the Results part.

III) Multi party mutual authentication

The propounded system facilitates several hospitals to get registered with the Global Hospital Server located at one city. This server stores the details of all the doctors and patients databases. All the patients are provided with an electronic data that contains their medical history and the relevant medical image shares as an encrypted image. Whenever the patient needs emergency medical help, he can approach any registered doctor available and get immediate medical help using this electronic image.

This Multi Party Authentication protocol is explained by the following steps of the Pseudo code:-

1) Patient submits his Pat_id, [Sh2||Pat_History].
2) Doctor desteganographs Pat_History from secret share 2, i.e., Sh2.
3) Doctor sends Doct_id, Pat_id, Sh2 to Global Hospital Server (GHS).
4) GHS checks the Doct_id for authenticity of the registration.
5) GHS server searches for Pat_id details and performs Visual Cryptographic Decryption on respective patient shares, Sh2, Sh1 to obtain processed endoscopic ulcer images.
6) GHS compares, with the original image and if matched,
7) GHS sends the recovered medical image of the patient to the registered doctor.
8) Doctor obtains the patients endoscopic ulcer image and based on the patient's history, he/she treats him/her, and also updates the history with the latest treatment details.

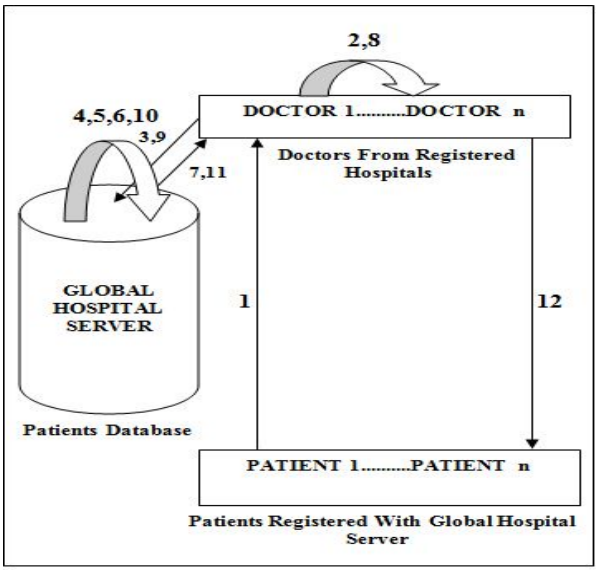

Figure-2. Mutual authentication diagram.

9) Doctor uploads the updated history and the medical image to the server (GHS).
10) The GHS again creates two secret shares and hides the updated history into SH2, while retaining SH1 in the server and sends SH2||updated Pat_History to doctor.
11) The doctor, receives respective patients updated SH2.
12) The doctor sends Pat_id||Sh2 to patient and logs out.

These steps are clearly depicted in the Figure-2.

4. RESULTS

We have implemented Matlab software R2010a for image processing and visual cryptographic encryption and decryption procedure. A considerable number of endoscopic ulcer images of various sizes have been taken for testing. The propounded scheme ensures effective encryption of shares and decryption. An endoscopic ulcer image is considered in Figure-3. Noise filtering technique i.e., median- filtering is implemented on such images containing peptic ulcers. The outcomes are displayed in the Figure-4.

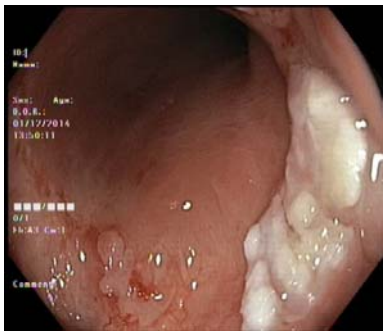

Figure-3. Endoscopic ulcer image.

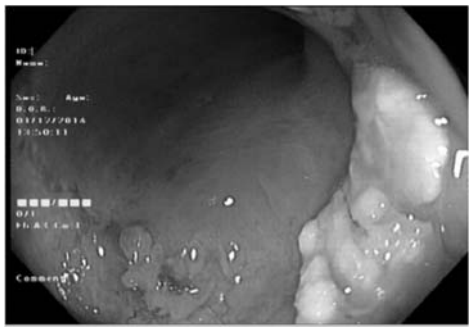

Figure-4. Outcome of median filtering.

The grow-cut segmented output of the above ulcer image is given below:

Figure-5. Outcome of grow cut segmentation.

It can be observed that the procured output image from grow-cut segmentation process, is not good in quality, but it is a standard one. The refining of the seed points are possible to improve the segmentation results based on the user's input. Once the image has been segmented by using grow-cut, these segmented images are half-toned, which are shown in Figure-6.

Figures 7 and 8 show the secret shares SH1 and SH2 patient data like doctor's name, patient's name, patient-id, D.O.B., sex, date of endoscopy, doctor's comments, treatment suggested are encrypted into the patient's secret share image by using steganographic method of encoding each character in the one of the corresponding pixels of the segmented endoscopic ulcer image Figure-9 shows the sample patient history that is to be steganographed. Figure-10 shows the stacked results obtained from stacking of secret share received from the server and the patient's side via the doctor. Figure-11 shows the multi party authentication results.

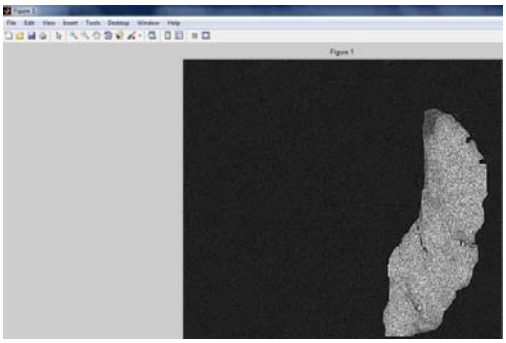

Figure-6. Patient secret image.

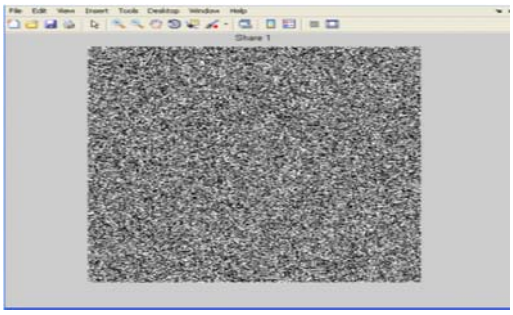

Figure-7. Secret share SH1.

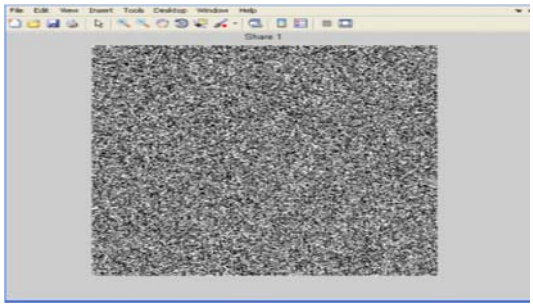

Figure-8. Secret share SH2.

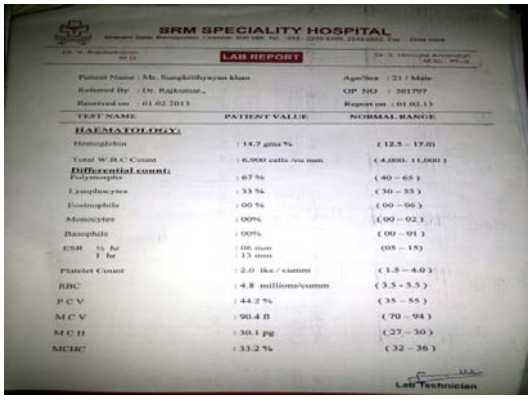

Figure-9. Sample patient history.

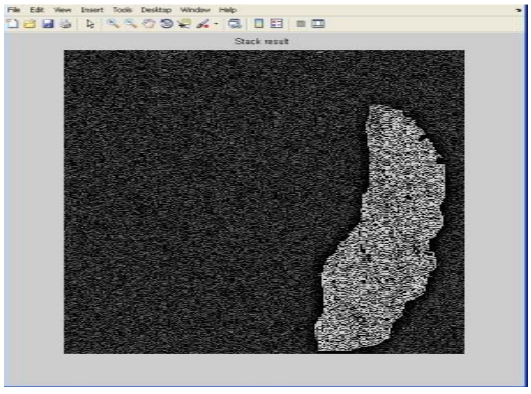

Figure-10. Stacked result.

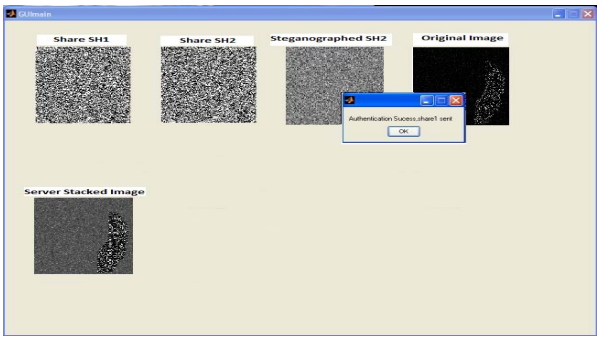

Figure-11. Results showing multi party server authentication.

5. CONCLUSION AND FUTURE WORKS

This particular paper deals with the multi party mutual authentication mainly for the patient database based on image processing techniques and visual cryptography protocols. The principle purpose of this propounded approach is that it overcomes the common problems of pixel expansion, and extra code-book needed for the purpose of stacking. The secret endoscopic ulcer image has also got the patient's history embedded into itself. The propounded approach ensures multi party mutual authentication by sending the patient's share of the secret image containing the details via the doctor to the global hospital server, where it gets verified. Random grid algorithm is used for share creation so as to overcome the problem of pixel expansion.

As a future enhancement of our propounded approach, mutual authentication can be implemented on different types of medical images, not only ulcer images, but this approach can be applied to ct scan images, etc. By implementing this propounded approach, the doctor's belonging to different hospitals can exchange numerous patient details encrypted with the shares in a more secured manner, thus helping the patients to get treatment from anywhere in the country, from any doctor, even without having the prescriptions.

ACKNOWLEDGEMENT

We are extremely grateful to the Sr. Consultant Gastroenterologist, Dr. B.S. Ramakrishna, MD, DM, PhD, FAMS, FNA of SRM Institutes for Medical Science for the support extended to us for this work in the field of ulcers. We are also grateful to Sr. Endoscopy Technician, Mr. C.V. Palanianandhan, DHCA, DET of SRM Institutes for Medical Science for guiding us in the field of endoscopy. We are also grateful to A. Vasuki, Assistant Professor, Department of ECE, SRM University for guiding us in the area of image processing. Without their help it would have been very hard to complete this work.

REFERENCES

[1] G. Coatrieux, H. Maître, B. Sankur, Y. Rolland, R. Collorec, "Relevance of Watermarking in Medical Imaging," in Proc. IEEE Int. Conf. ITAB, USA, pp. 250-255, 2000.

[2] Boykov Y., Veksler O., Zabih R., "Fast approximate energy minimization via graph cuts".

[3] Grady L., Funka-Lea G., "Multi-label image segmentation for medical applications based on graph-theoretic electrical potentials". In ECCV Workshops CVAMIA and MMBIA, 230-245, 2004.

[4] Baykov Y., Jolly M. P., "Interactive graph cuts for optimal boundary and region segmentation of objects in n-d images." 2001.

[5] B. Chen and G.W. Wornell, "Quantization Index Modulation: A Class of Provably Good Methods for Digital Watermarking and Information Embedding,' IEEE Trans. Information Theory. Vol. 47, No. 4, pp. 1423-1442, 2001

[6] N. Provos and P. Honeyman, "Hide and Seek: An Introduction to Steganography", IEEE Security and Privacy, pp. 32-44, May/June 2003.

[7] Y. Boykov and M.-P. Jolly, Interactive organ segmentation using graph cuts. "In Medical Image Computing and Computer-Assisted Intervention", pp. 276-286, 2000.

[8] Carsten Rother, et al, GrabCut -Interactive Foreground Extraction using Iterated Graph Cuts, ACM Transactions on Graphics (SIGGRAPH), 2004.

[9] N.G. Kingsbury, "Complex wavelets for shift invariant analysis and filtering of signals," in Journal of Applied and Computational Harmonic Analysis, vol. 10, no. 3, pp. 234–253, May 2001.

[10] Jianbo Shi and Jitendra Malik, "Normalized Cuts and Image Segmentation", IEEE Transactions on pattern analysis and machine intelligence, pp. 888-905, Vol. 22, No. 8, 2000.

[11] B. Borchert, .Segment Based Visual Cryptography. WSI Press, Germany, 2007.

[12] Leo Grady, "Random Walks for Image Segmentation", IEEE Transactions on Pattern Analysis and Machine Intelligence, pp. 1768-1783, Vol. 28, No. 1, 2006.

[13] W-Q Yan, D. Jin and M. S. Kanakanahalli, .Visual Cryptography forPrint and Scan Applications. IEEE Transactions, ISCAS-2004, pp. 572-575.

[14] T. Monoth and A. P. Babu, .Recursive Visual Cryptography Using Random Basis Column Pixel Expansion. In Proceedings of IEEE International Conference on Information Technology, 2007, pp. 41-43.

[15] H. J. Kim, V. Sachnev, S. J. Choi and S. Xiang, .An Innocuous Visual Cryptography Scheme. In Proceedings of IEEE-8th International Workshop on Image Analysis for Multimedia Interactive Services, 2007.

[16] M. A. Dorairangaswamy, "A Novel Invisible and Blind Watermarking Scheme for Copyright Protection of Digital Images," International Journal of Computer Science and Network Security (IJCSNS), Vol. 9, No. 4, pp. 71-78, 2009.

[17] A.Dorairangaswamy, B.Padhmavathi, "An Effective Blind Watermarking Scheme for Protecting Rightful Ownership of Digital Images, Proceedings IEEE Conference. TENCON 2009, Vol. 1.

[18] Wen-Pinn Fang,"Non-expansion Visual Secret Sharing in Reversible Style", IJCSNS, Vol. 9 No.2, February 2009.

[19] Wen-Pinn Fang, "Visual Cryptography in reversible style,"IEEE Proceeding on the Third International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIHMSP2007), Kaohsiung, Taiwan, R.O.C, 2007, 11, 26～2007, 11, 28.