Facilitating and securing offline e-medicine service through image steganography

A.H.M. Kamal[1,2], *M. Mahfuzul Islam*[2]

[1]*Department of Computer Science and Engineering, Jatiya Kabi Kazi Nazrul Islam University, Mymensingh, Bangladesh*
[2]*Department of Computer Science and Engineering, Bangladesh University of Engineering and Technology, Bangladesh*
E-mail: ahmkctg@yahoo.com

Published in Healthcare Technology Letters; Received on 4th November 2013; Revised on 3rd May 2014; Accepted on 6th May 2014

E-medicine is a process to provide health care services to people using the Internet or any networking technology. In this Letter, a new idea is proposed to model the physical structure of the e-medicine system to better provide offline health care services. Smart cards are used to authenticate the user singly. A very unique technique is also suggested to verify the card owner's identity and to embed secret data to the card while providing patients' reports either at booths or at the e-medicine server system. The simulation results of card authentication and embedding procedure justify the proposed implementation.

1. Introduction: Communication with secret data is always challenging. Exchanging data between two systems, that is, computers, mobile nodes or terminals and smart cards through the Internet or any networking technology maintaining integrity and confidentiality is a difficult task. Of the commonly used security policies, three well-known methods are encryption, watermarking and steganography. The basic limitation of encryption is that one can presume the existence and try guessing key(s) or portion of message to retrieve secret data. Again although watermarking conceals a message inside an image, it exhibits [1, 2] the secret data to all. It does nothing but prohibits the alteration of data only. As for steganography, it befools the intruder by hiding the very existence of secret data.

Steganography is an art of embedding data to a cover medium in such a way that the intruder cannot guess the existence of those data within it. This process to communicate with secret data between two systems can also be used in e-medicine. E-medicine is a system where treatments to the patient can be offered through communication technology. The services of e-medicine can be ensured online or offline. In online services, patients will enjoy a live communication with the doctor, and under the offline system, patients will submit their queries to a server seeking a doctor's consultancy that would be offered later. Traditionally in both cases, the symptoms, diagnosis and reports of patients' diseases are delivered through insecure channels. This always threatens the confidentiality and integrity of patients' data [3]. Here comes the great use of steganography, if associated to the e-medicine system. In that procedure, e-medicine process necessitates two components: modelling the system and applying a method for the steganographic process.

Modelling the system for the online process is easier and less expensive than for the offline process. At the online system, patients having a computer or any such mobile node connected to the doctor can use the telemedicine facility. The offline system, contrariwise, require several booths assembled with a module to receive symptoms from the patients and to embed those to reports or images and even to manage those according to user IDs to a database. The booth again collects the consulted reports from doctors and presents those to the patients. The patients are identified by their password and biometrics. Another module at the server manages the distributions of patients' queries to the right specialists and the specialists' responses thereon. A smart card named 'medical card' is used to login to the booth. Modelling such system is described in Section 2.

The cover media used at the booth to embed symptoms are usually images, text, audio or video data [4–6]. Of those all, images are widely used for their size, redundant data and very frequently transmitted manner over the Internet for regular purposes [6]. An algorithm is used to conceal message bits within the pixel values of the image known as the 'carrier' or 'the cover image'. The image that contains the embedded message is called 'stego image' which is next transmitted to the destination. A pictorial view of that process is given in Fig. 1.

The depicted steganography process is used to personalise a medical card, to authenticate a smart card [7] at the terminal, and to hide symptoms to reports. Smart cards like debit or credit cards, personal identification cards at an office, national cards, among others, are very much famous for their flexible portability and multipurpose uses. Such cards make life easier, and people are accepting those rapidly. Hence using a smart card as a medical card is preferred. However, the risks are also increasing as the card can be stolen or lost. So then the confidentiality and personality of a user cannot be maintained, and moreover prohibiting unwanted service charges can also be demolished. Usually, smart cards use very old encryption methods for their simplicity, faster processing, lower use of memory and easier implementation. That encryption standard has increased risk factors as nowadays breaking such security has become a matter of few minutes. To increase the reliability hash functions are employed along with encryptions [8–13]. However, for encryption exponents and larger hashing keys, the computational complexity becomes noticeable. As an alternative to encryption and hashing, applying steganography can then be an appropriate selection. Password and biometric parameters can be embedded to the image of the card owner. That image can then be installed to the chip of the card.

Brindha and Vennila [7] proposed a method of using the image steganography technique for hiding the fingerprint of a person inside his face image for smart card authentication. It is a completely new area of applying image steganography. However, the use of the least significant bit (LSB) replacement algorithm has made the policy weaker [1]. Applying chi-square test, it is possible to detect the possibility of existence of embedded data. Another application by Pang *et al.* [14] is seen to maintain the privacy of electronic voting. A similar application is also presented in the literature by Rura *et al.* [15]. These applications differ a bit with smart card applications. For smart cards, authentication is done with the terminal for the card.

In this Letter, modelling e-medicine system and its technical issues are demonstrated. To the best of our knowledge, such modelling and embedding techniques are unique. This Letter includes five more sections. Section 2 illustrates the model of e-medicine and thereafter, in Section 3, embedding policies are explained. Sections 4 and 5 present a performance comparison of the proposed

doi: 10.1049/htl.2013.0026

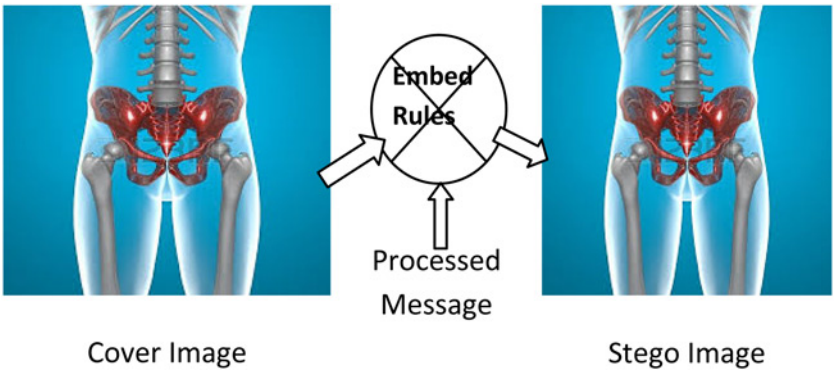

Figure 1 *Image steganography*

scheme with others and the effectiveness of the proposed one against statistical attacks, respectively, whereas Section 6 closes this Letter with a concluding remark.

2. Modelling the system: To ensure e-medicine facilities at rural and urban areas and to support mass people, the offline system is preferable and hence it is demonstrated here. The proposed offline system is depicted in Fig. 2. The model consists of several booths located at different places of the cities. Each booth contains two modules. One is to authenticate the medical card and another is to hide symptoms and other data to the reports or photographs of patients. Medical cards are issued by hospital authorities. Before issuing the card, the photograph of the card owner containing embedded login information is stored into the chip of the card. A user ID and a secret code are handed over to each user. The card registration process is shown in Fig. 4.

Each terminal, or booth, first authenticates the card. The authentication process is explained in the following section. If the card owner is verified successfully, he goes through several steps to present all symptoms to the terminal. The terminal also asks for a photograph or the medical reports (otherwise a sample image will be chosen from the internal database) to be uploaded. Then all the accepted information is concealed inside that photograph or medical reports. Those are transmitted to the server of the system. The server analyses the symptoms and categorises the problem as skin, sex, ear, heart, eye, throat, head, child, gynecology and so on. The system then assigns the problem to the respective specialists maintaining a chronological distribution. It grabs a problem from the pool and assigns it to one doctor; again grabs another problem and assigns to the second doctor and so on.

After obtaining feedback from the doctor, the consulted report is again embedded to a photograph by the server which is thereafter delivered to the patient upon a further request by the patient from a booth.

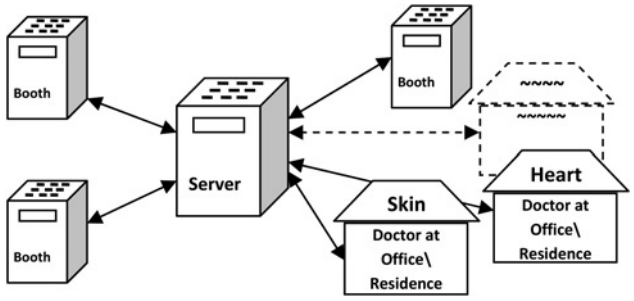

Figure 2 *System block of e-medicine*

3. Embedding and extracting procedure: Security affairs in smart cards are vital issues. To improve security of smart cards, use of steganography is the latest concept of its type. As the smart card uses less memory and a low computational power processor compared to a laptop, least significant bit replacement algorithms are commonly used. To improve the security of embedded data Brindha and Vennila [7] have proposed to use scattered LSB embedding algorithm. However, the chi-square test from Liu and Liao [16] and vertical and horizontal difference histogram from Zhao *et al.* can detect the possibility of the existence of embedded data in an image [5]. Therefore to enhance the security a new approach is explained here.

3.1. Objective function: The proposed method simultaneously uses some non-overlapping functions like f_1, f_2, ..., f_n to embed data. Those functions are used to select the pixels from the image. At a time each function can select one pixel and the tern of each function depends on the selection of a row from a set of possibilities listed in Table 2. For example, if the sequence f_1, f_2, …, f_n is chosen, the first pixel is selected by f_1, the second pixel is selected by f_2 and so on until f_n is applied. Then again the process starts applying f_1 first. Those functions are called objective functions. Some of the examples of such functions are rectangle, triangle, polygon, circle, oval, parabola, line, sinc and so on. Four of those are depicted in Fig. 3.

Each function has its own parameters. Table 1 shows the list of parameters that are used by each function.

Those functions are used only to select pixels from grid positions (x, y). The third column of the table shows the start and progress path of each function. Then simple LSB replacement algorithms are used to embed data. To reduce the complexity, uses of four functions, f_1, f_2, f_3 and f_4, for each user are described. Those are

Table 1 Parameters used by functions

Function	List of parameters	Start and progress path of each function
circle	centre (x_0, y_0), radius r, theta θ and step Δ	start: θ = 0 progress: scan by θ + Δ
rectangle	points: top left (x_1, y_1) and right bottom (x_2, y_2)	start: left vertical line progress: loop clock wise
triangle	corner points: (x_3, y_3), (x_4, y_4) and (x_5, y_5)	start: line (x_3, y_3, x_4, y_4) progress: loop clock wise
line	end points: (x_6, y_6) and (x_7, y_7)	start: (x_6, y_6) progress: scan line.
polygon	corner points: (x_8, y_8), (x_9, y_9), … , (x_n, y_n)	start: line (x_8, y_8, x_9, y_9) progress: loop clock wise
sinc	constant n and π and theta θ, step Δ	start: θ = 0 progress: θ + Δ

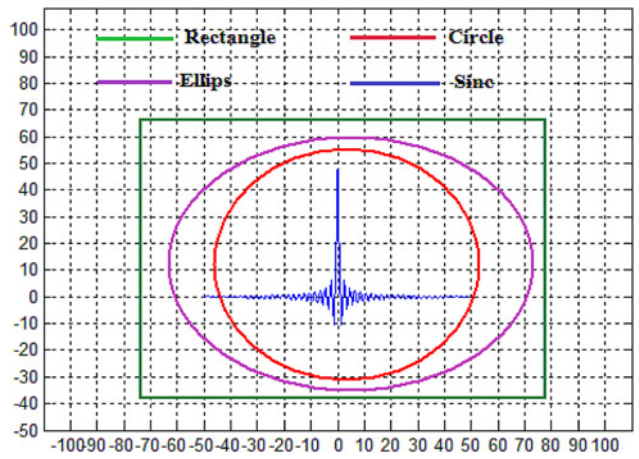

Figure 3 *Some of the objective functions*

permuted to prepare a list of function's sequences which are shown in Table 2 and stored at the server.

3.2. Values of parameters of functions: Functions do not contain the same value for all the users. The values come from a predefined list, also tabulated in Table 3 and are stored at the server.

By arranging parameters in random order, values are assigned to those. Those values are fixed for the parameters for selected *ParamVal*. For example, if 4 as a value of *ParamVal* is given to the terminal, it will consider the values as $\{x_1, y_1, r, \theta, \Delta, x_2, y_2, \ldots\} = \{10, 10, 130, 5^0, 10^0, \ldots\}$. Based on those values the terminal will extract the embedded information. This *ParamVal* is a part of user's secret code. However, it may differ for other users.

3.3. LSB replacement algorithm: In smart cards, distortion of the image quality is not a very important issue to consider because the image is not sent over the Internet or a network. However, the images or reports that contain embedded symptoms are sent to a server over public network. Hence to preserve the visual quality fewer LSBs should be replaced. The LSB replacement algorithm is not explained here as the proposed Letter does not modify the LSB replacement algorithm in [17, 18].

3.4. Card registration and verification process: All the users will be given a password to operate the card. Client passwords will carry some secret information. Passwords will consist of user *ID*, *PermSec*, *ParamVal*, that is, *Password* = *ID* ||*PermSec*|| *ParamVal* where || is a concatenation symbol.

Before providing the password, the hospital authority needs to install the card with required information. They will embed the secret information to the photograph of the user and then install it to a proper location into the card. This way the client will complete the registration process shown in Fig. 4.

Next when the client pushes it into the terminal, it will read the photograph and then extract the embedded information to verify the identity. The process is explained as follows:

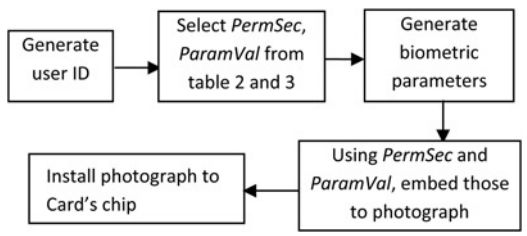

Figure 4 *Card registration*

Table 2 Possible sequences of applying functions at embedding

PermSec	Function sequence	*PermSec*	Function sequence
1	f_1, f_2, f_3, f_4	12	f_3, f_1, f_2, f_4
…	…	…	…
6	f_1, f_4, f_3, f_2	18	f_3, f_4, f_2, f_1
7	f_2, f_1, f_3, f_4	19	f_4, f_1, f_2, f_3
…	…	…	…
12	f_2, f_4, f_3, f_2	24	f_4, f_3, f_2, f_1

i. Push the card into the terminal.
ii. The terminal will read the photograph.
iii. It will ask the user to provide the password.
iv. The terminal will separate the values of *PermSec* and *ParamVal* from the password.
v. It will then retrieve objective functions and values of parameters as shown in Tables 2 and 3.
vi. The terminal will extract the information from the image.
vii. It will compare the extracted *ID* with the given *ID*.
viii. If both *IDs* are same, the user is allowed to seek for consultancy.
ix. Reject otherwise.

The *ID* consists of 4 digits (may be extended if it is required) and *PermSec* consists of two digits. *ParamVal* will be from 0 to 99. So the length of the password is 8 digits which is long enough but easy to remember.

Based on those *PermSec* and *ParamVal*, the user *ID* and other information like biometrics are embedded into the image of the card owner by the authority.

3.5. Extraction and user verification: After receiving the smart card, the terminal will ask for a password and biometric information. Receiving those from the client, the terminal will process the given biometrics to find parameters like minutia for finger print. Then it will decompose the password to find *PermSec* and *ParamVal* values. Based on those values, it will define the application sequence of functions and their parameters' values. Now it is ready to extract hidden information. The terminal will calculate the value (x, y) for the first function. After that it will extract m-bits LSB from the pixel of grid position (x, y). That will continue for the other three functions and circularly the process will be continued until all embedded information is extracted.

At that stage, it will compare the *ID* with the extracted *ID*, the biometric parameters with the extracted biometric parameters. So the security is very strong here. The scenario is depicted in Fig. 5.

4. Performance comparison with related scheme: In this section, the scheme of Das [8], Liao *et al.* [9], Yoon *et al.* [10], Liou *et al.* [11], Wang *et al.* [12] and Khan *et al.* [13] are compared with the proposed technique. All the schemes undergo three phases: registration, login and authentication to put the card into

Table 3 Parameters list and assigned values

ParamVal	Parameter list	Value of parameter (example)
1	$\{\Delta, \theta, r, x_1, y_1, x_2, y_2, \ldots\}$	$\{10^0, 0^0, 120, \ldots\}$
2	$\{\theta, \Delta, r, x_1, y_1, x_2, y_2, \ldots\}$	$\{10^0, 5^0, 115, \ldots\}$
3	$\{r, \theta, \Delta, x_1, y_1, x_2, y_2, \ldots\}$	$\{125, 5^0, 15^0, \ldots\}$
4	$\{x_1, y_1, r, \theta, \Delta, x_2, y_2, \ldots\}$	$\{10, 10, 130, 5^0, 10^0, \ldots\}$
…	…	….
…	…	….

doi: 10.1049/htl.2013.0026

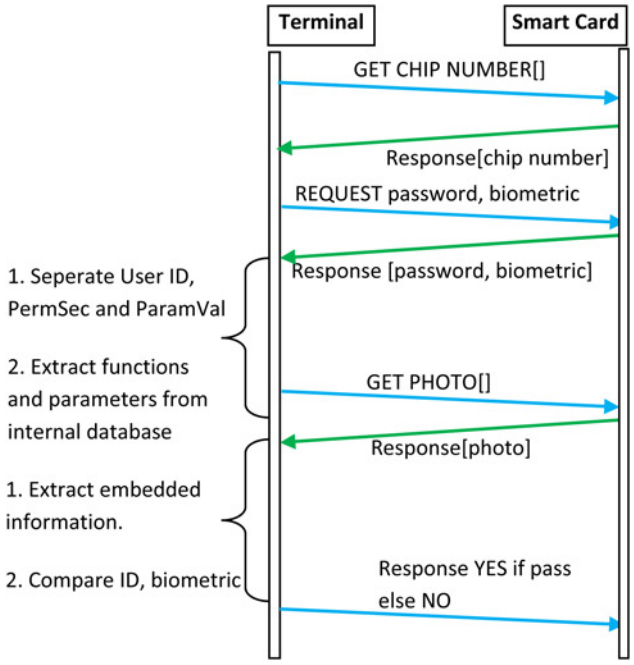

Figure 5 *Card verification*

operation. At the registration phase, all the schemes compute a hash value from a list of parameters like random numbers, ID, password, biometrics and secret keys. The card is personalised by a hash value, hash function and a secret key. At the same phase the proposed scheme differs from all the others by personalising the card through embedding a password and biometrics into the photograph stored in it. No secret keys of a remote server and no hash function are used there. That is why the computational complexity is less compared with others because computing hash and exponentials is more time-consuming issues than accessing a matrix sequentially. At login time, all the schemes compute another hash value which is called 'login code', while the proposed scheme computes biometric parameters from given biometrics. Again at the authentication phase, the terminal computes another hash and compares it to the login code to verify the client, whereas the proposed scheme extracts biometric information and the password from the photograph and compares those to the user-provided password and biometrics. A performance comparison is listed in Table 4.

From the table, it is observed that all the methods use at least ten numbers of hashes, a fact which increases the time complexity of the computation. Moreover, all the stated schemes except the proposed one perform a good number of bitwise XOR operations and concatenation of string too. For simplicity those are ignored. On the other hand, the proposed scheme finds *PermSec* and *ParamVal* by 2 hits only from Tables 2 and 3 and then it embeds

Table 4 Comparison of computational performance

Schemes	Registration	Login and verification	Total
Liao *et al.* [9]	2H	9H	11H
Yoon *et al.* [10]	3H	10H	13H
Liou *et al.* [11]	3H	9H	12H
Wang *et al.* [12]	2H	8H	10H
Khan *et al.* [13]	3H	10H	13H
Das [8]	3H + 1B	7H + 1B	10H + 2B
proposed	2 + 1S + 1B	1S + 1B	2 + 2S + 2B

H: One-way hash function, S: Steganograpy and B: Compute biometric parameters.

the 32 bits password and L bits biometric information (total $32 + L$ bits) to the card and extracts the same at the verification phase from an image of the size 80×80 (so complexity depends on L which must be less than $2 + 80 \times 80$). Hence the embedding and extraction time for $32 + L$ bits from an image is very negligible compared with biometric calculations along with hybrid uses of hashes, XORs and concatenations operations in other schemes.

5. Resistance of proposed scheme against statistical attack: In the proposed scheme, the password and biometrics consisting of $32 + L$ bits are embedded to a passport size photograph of the card owner. Hence the alteration of image data is too small to be realised either visually or statistically. Moreover, the photograph will reside permanently in the card. Hence security issues are not a major concern here. On the other hand, the patient's symptoms are embedded to reports or a sample image which can be a bit longer than $32 + L$ bits; however, those are not too much. Rather it can be said that very few data are embedded by the terminal. Hence, the embedding capacity is not a major concern there. Owing to the embedding requirement of fewer bits, the visual quality of the report or the photograph will not be changed noticeably. Therefore experiments are done to test the resistance against the statistical attacks only.

5.1. Applying chi-square test: The chi-square test [16], is a very common method to detect the embedded data by LSB replacement. Chi-square on $m \times n$ image was applied based on the following relation

$$X^2 = \sum_{i=1}^{m} \sum_{j=1}^{n} \frac{O_{i,j} - E_{i,j}}{E_{i,j}} \tag{1}$$

Here, $O_{i,j}$ represents the pixel values of the stego image and those can also be termed as observed values whereas $E_{i,j}$ represents the values of pixels of the cover image and can also be termed as expected values. Then it infers the degree of freedom, DF by $\mathrm{DF} = (m-1)^*(n-1)$. Here DF is much greater than 30. So normal distribution is used as chi-square statistics which can be measured from

$$\sqrt{X^2} - \sqrt{2\mathrm{DF} - 1} \tag{2}$$

Those values are tested against critical chi values. MATLAB tool chi2inv is used to measure the critical value X^2_{α} setting the probability at 0.005. Fig. 6 shows that chi-square values are negligible with respect to chi critical values. To make sense of the comparison, a logarithm of chi values and critical values is used. So it can be concluded that the test results successfully pass the chi-square test.

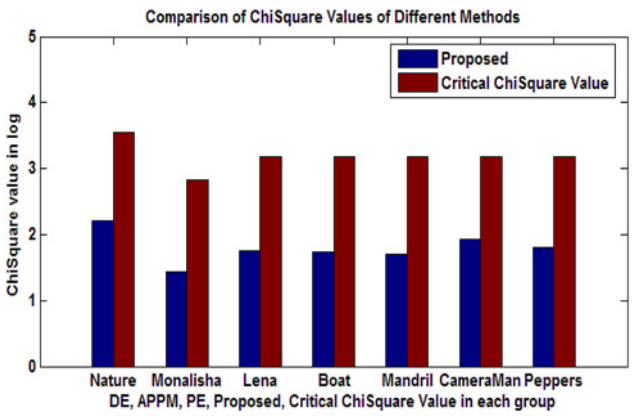

Figure 6 *Result of chi-square statistics*

5.2. Vertical and horizontal difference histogram: Pixel values of a natural image usually maintain a correlation with neighbours while a tempered image can exhibit abnormality which can be checked by steganalysis of complementary embedding [19]. Another interesting methodology to detect hidden information from vertical and horizontal difference histogram was proposed by Zhao *et al.* [20] and its applications are outlined in various literatures [17, 21, 22]. In our experiment horizontal difference histogram $\check{H}_{\mathrm{h}}$ and vertical difference histogram $\check{H}_{\mathrm{v}}$ are measured first from a stego image. Then the summation of the square root of the differences of those two histograms produces a very small value for natural images. The equation is shown as follows

$$D = \left(\sum_{i=-T}^{T} (\check{H}_{\mathrm{h}}(i) - \check{H}_{\mathrm{v}}(i)) \right)^{1/2} \tag{3}$$

Here T is a threshold. In our test T was set to 40.

The highest value of D for some images was found to be 120 and the lowest 10. The experimental result is depicted in Fig. 7. It can be observed that at Fig 7*a*, for one bit embedment per pixel, the curve of $\check{H}_{\mathrm{h}}$ and $\check{H}_{\mathrm{v}}$ are depicting synchronised behaviour while Fig. 7*b* is exhibiting some abnormalities because of 3 bits embedment per pixel. Hence, it can be resolute that embedding more bits per pixel will generate more distortion [23]. However, in e-medicine, the numbers of bits to be embedded are remarkably fewer than the image size. Therefore single bit embedment per pixel is enough to support the patient demands.

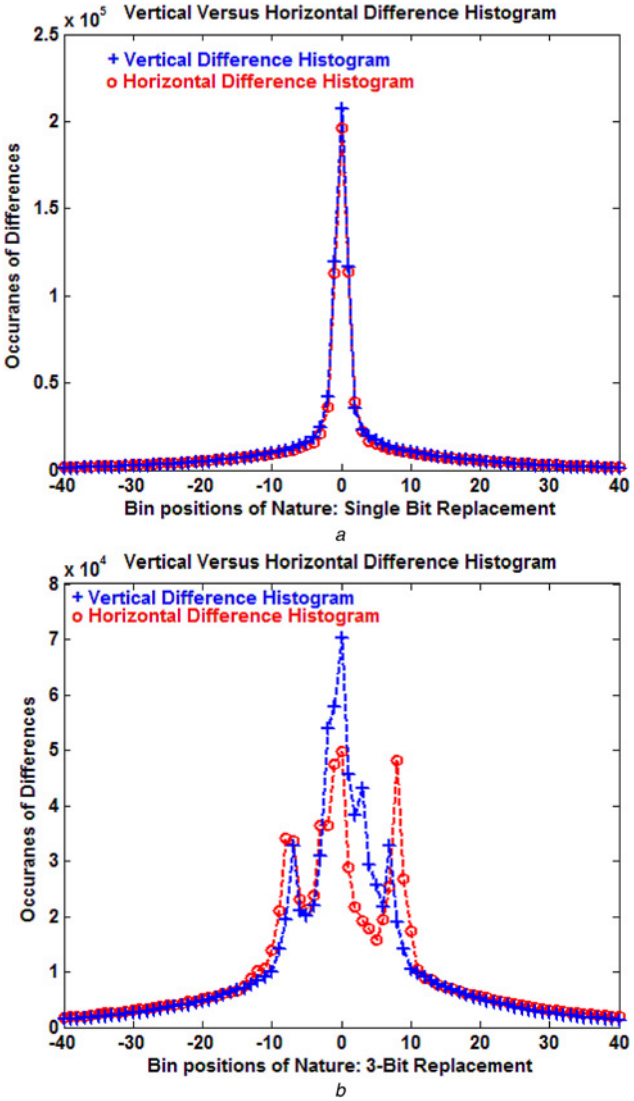

Figure 7 *Comparison of vertical difference histogram and horizontal difference histogram*
a 1-bit replacement
b 3-bit replacement

6. Conclusions: Smart card authentication through embedded data is a new arena of image steganography. The proposed scheme successfully shows that steganography can be applied to increase the reliability of uses of smart cards. What makes the proposed scheme robust are multiple functions, their various applying sequences and possibilities of assigning different values for parameters in different cards. Our scheme can notably contribute to the secure authentication of smart cards as well as to the research area of image steganography.

The modelling of the physical structure of an e-medicine system is also a unique proposal. Such a system will bring the medical service to the door of people. Besides, treatment directly sent to remote villages from skilled and specialised urban doctors will obviously increase the health service of the government of a nation. People of all nations will benefit from the system.

In our future endeavour, we hope to offer a login booth from a mobile phone. In that case, mobile numbers will also be registered to the server upon the request of clients. Next upon receiving any request from a mobile node of a client, the terminal will fetch the stego photograph from the server of the e-medicine system by the client's ID. This type of communication can be done through multimedia messaging service. Finally, the terminal will compare the extracted biometrics, the ID and the password from the stego photograph with the received biometrics, the ID and the password through a mobile phone. This way authentication can be carried out using mobile phones. Then people will have their own booth at their hand constantly.

7. Acknowledgments: This Letter is an outcome of PhD research. The authors are thankful to all of their colleagues and members of the research group for their encouragement. A special thanks to Mr. Md. Wasiuzzaman, Assistant Professor, Dept. of English Language and Literature of Jatiya Kabi Kazi Nazrul Islam University, Mymensingh, Bangladesh for his help with the formatting of this Letter.

8 References

[1] Chen C.-C., Tsai Y.-H.: 'Adaptive reversible image watermarking scheme', *J. Syst. Softw.*, 2011, **84**, (3), pp. 428–434
[2] Kamstra L., Heijmans H.J.: 'Reversible data embedding into images using wavelet techniques and sorting', *IEEE Trans. Image Process.*, 2005, **14**, (12), pp. 2082–2090
[3] Ulutas M., Ulutas G., Nabiyev V.V.: 'Medical image security and EPR hiding using Shamir's secret sharing scheme', *J. Syst. Softw.*, 2011, **84**, (3), pp. 341–353
[4] Lee C.-F., Chen H.-L.: 'A novel data hiding scheme based on modulus function', *J. Syst. Softw.*, 2010, **83**, (5), pp. 832–843
[5] Tian H., Zhou K., Hong J., *ET AL.*: 'An M-sequence based steganography model for voice over IP'. IEEE Int. Conf. on Communications (ICC 2009), 2009
[6] Provos N., Honeyman P.: 'Hide and seek: an introduction to steganography', *IEEE Secur. Priv.*, 2003, **1.3**, pp. 32–44
[7] Brindha S., Vennila I.: 'Hiding fingerprint in face using scattered LSB embedding steganographic technique for smart card based authentication system', *Int. J. Comput. Appl.*, 2011, **26**, (10), pp. 51–55
[8] Das A.K.: 'Analysis and improvement on an efficient biometric-based remote user authentication scheme using smart cards', *IET Inf. Secur.*, 2011, **5.3**, pp. 145–151
[9] Liao I., Lee C.C., Hwang M.S.: 'Security enhancement for a dynamic ID-based remote user authentication scheme'. Proc. of the Int. Conf. on Next Generation Web Services Practices (NWeSP'05), Seoul Korea, 2005, pp. 437–40
[10] Yoon E.J., Ryu E.K., Yoo K.Y.: 'An improvement of Hwang-Lee-Tang's simple remote user authentication schemes', *Comput. Secur.*, 2005, **24**, pp. 50–6

doi: 10.1049/htl.2013.0026

[11] Liou Y.P., Lin J., Wang S.S.: 'A new dynamic ID-based remote user authentication scheme using smart cards'. Proc. of 16th Information Security Conf. 2006, Taiwan, pp. 198–205
[12] Wang Y.Y., Kiu J.Y., Xiao F.X., Dan J.: 'A more efficient and secure dynamic ID based remote user authentication scheme', *Comput. Commun.*, 2009, **32**, (4), pp. 583–5
[13] Khan M.K., Kim S.K., Alghathbar K.: 'Cryptanalysis and security enhancement of a more efficient & secure dynamic ID-based remote user authentication scheme', *Comput. Commun.*, 2011, **34**, pp. 305–9
[14] Pang L., Sun M.-H., Luo S.-S., *ET AL.*: 'Full privacy preserving electronic voting scheme', *J. China Univ. Posts Telecommun.*, 2012, **19**, (4), pp. 86–93
[15] Rura L., Issac B., Haldar M.K.: 'Secure electronic voting system based on image steganography'. 2011 IEEE Conf. on Open Systems (ICOS 2011), 2011
[16] Liu C.-L., Liao S.-R.: 'High-performance JPEG steganography using complementary embedding strategy', *Pattern Recognit.*, 2008, **41**, (9), pp. 2945–2955
[17] Hong W., Chen T.-S., Luo C.-W.: 'Data embedding using pixel value differencing and diamond encoding with multiple-base notational system', *J. Syst. Softw.*, 2012, **85**, (5), pp. 1166–1175
[18] Yang C.-H., Weng C.-Y., Wang S.-J., Sun H.-M.: 'Varied PVD + LSB evading detection programs to spatial domain in data embedding systems', *J. Syst. Softw.*, 2010, **83**, (10), pp. 1635–1643
[19] Huang F., Luo W., Huang J.: 'Steganalysis of JPEG steganography with complementary embedding strategy', *IET Inf. Secur.*, 2011, **5**, (1), pp. 10–18
[20] Zhao H., Wang H., Khan M.K.: 'Statistical analysis of several reversible data hiding algorithms'. Proc. Multimedia Tools and Applications, 2009, DOI: 10.1007/s11042-009-0380-y
[21] Hong W., Chen T.-S.: 'A novel data embedding method using adaptive pixel pair matching', *IEEE Transactions on Information Forensics and Security*, 2012, **7.1**, pp. 176–184
[22] Hong W., Chen T.-S.: 'A local variance-controlled reversible data hiding method using prediction and histogram-shifting', *J. Syst. Softw.*, 2010, **83.12**, pp. 2653–2663
[23] Lin C.-C.: 'An information hiding scheme with minimal image distortion', *Comput. Stand. Interfaces*, 2011, **33**, (5), pp. 477–484