SECURE COMMUNICATION USING ADAPTIVE PIXEL PAIR MATCHING EMBEDDING METHOD AND NYMBLE SYSTEM

Seethal Thomas
PG Student
K.S.R.College of Engineering
Thiruchengode
Phone no.:09496720175

Mr.R.Eswaramoorthi
Assistant professor
K.S.R.College of Engineering
Thiruchengode
Phone no.:09865653985

ABSTRACT

A secure communication using adaptive pixel pair matching (APPM) embedding method and nymble system is proposed. The data to be secured is made hidden using APPM method and then saved from where only authorised entities can access the file. The basic idea of pixel pair matching (PPM) is to use the values of pixel pair as a reference coordinate, and then search a coordinate in the neighbourhood set of the reference coordinate according to a given message digit. The pixel pair is then swapped by the searched coordinate to conceal the digit. The two data-hiding methods proposed recently based on PPM are Exploiting modification direction (EMD) and diamond encoding (DE). Diamond encoding is the extension of EMD whereas the APPM method is the extension of DE. The proposed method offers lower distortion than DE and other steganographic methods, by providing more compact neighbourhood sets and allowing embedded digits in any notational system. To provide more security to the hidden data, we present Nymble, a system in which servers can blacklist misbehaving users in the network, thereby blocking users without compromising their anonymity. Thus the proposed system ensures that the data to be communicated is more secure

Key words: Adaptive pixel pair matching (APPM), diamond encoding (DE), exploiting modification direction (EMD), least significant bit (LSB), optimal pixel adjustment process (OPAP), pixel pair matching (PPM), Nymble, Anonymous blacklisting, privacy.

INTRODUCTION

Nowadays digital communication has become an essential part of communication infrastructure. The number of internet based applications is highly progressing. Therefore it is essential to secure the information that is passed over an open channel. The confidentiality and data integrity are required to protect against unauthorized access and use. This has

resulted in an unstable growth in the field of information hiding. Steganography is the science that involves communicating secret data using appropriate multimedia carrier like image, audio, and video files. It transforms the carrier in an unrevealed way only so that it reveals nothing neither the embedding of a message nor the embedded message itself. The recent development of the Internet has brought new attention to steganography. The interest in steganography has been enhanced recently by the emergence of commercial espionage and the growing concerns about homeland security due to terrorism. The purpose of steganography is therefore to hide a secret message in a carrier. With the enhancement in computer power, the internet and with the development of digital signal processing, information theory and coding theory, steganography has gone digital. In this digital world steganography has created an atmosphere of corporate vigilance that has spawned various applications, thus its continuing evolution is assured. Steganography is employed in various useful applications, such as advanced data structures, medical imagery, strong watermarks, military agencies, intelligence agencies, document tracking tools, document authentication, general communication, digital elections and electronic money, radar systems and remote sensing. Steganography's ultimate objectives and the main factors that separate it from related techniques such as watermarking and cryptography are undetectability, robustness and capacity of the hidden data.

Though we hide information using steganographic methods, there are probabilities of information being hacked by the misbehaving users when it is delivered through the internet. Nymble system can be used to solve this issue. The purpose of the Nymble is to allow for responsible, anonymous access online. It provides a mechanism for server administrators to block misbehaving users while allowing for honest users to stay anonymous. By providing a mechanism for server administrators to block anonymous misbehaving users, we can make the anonymizing networks such as Tor more acceptable for server administrators everywhere.

RELATED WORK

The least significant bit substitution method, referred to as (LSB), is a well-known data-hiding method. In LSB embedding, the pixels with even values will be increased by one or kept unchanged. The pixels with odd values will be decreased by one or kept unmodified. Therefore, the unfair embedding distortion emerges and is vulnerable to steganalysis. In 2004, Chan *et al.* [8] proposed a simple and efficient optimal pixel adjustment process (OPAP) method to reduce the distortion caused by LSB replacement. The LSB and OPAP methods employ one pixel as an embedding unit, and conceal data into the right-most LSBs. There are other data-hiding methods that employ two pixels as an embedding unit to conceal a message digit in a B-ary notational system. These data-hiding methods are termed as pixel pair matching (PPM). In 2006, Mielikainenproposed an LSB matching method based on PPM. He used two pixels as an embedding unit. The LSB of the first pixel is used for carrying one message bit, while a binary function is employed to carry another bit. In Mielikainen's method, two bits are carried by two pixels. There is a 3/4 chance a pixel value has to be changed by one yet another 1/4 chance no pixel has to be modified[9] .In 2006, Zhang and Wang [10] proposed an exploiting modification direction (EMD) method. To enhance the image quality of EMD, Wang *et al.* [5] in 2010 proposed a novel section-wise exploring modification direction method. EMD improves Mielikainen's method in which only one pixel

in a pixel pair is changed one gray-scale unit at most and a message digit in a 5-ary notational system can be embedded. The embedding method of LSB matching and EMD offers no mechanism to increase the payload.

In 2009, Chao *et al.* [12] proposed a diamond encoding (DE) method to enhance the payload of EMD further. DE employs an extraction function to generate diamond characteristic values (DCV), and embedding is done by modifying the pixel pairs in the cover image according to their DCV's neighbourhood set and the given message digit

In pseudonym Systems, an individual will be known to other users by a pseudonym which is blacklisted if a user misbehaves. But this results in pseudonymity for all users and weakens the anonymity. Also the users should be prevented from sharing their pseudonyms. Group signature[14] is a method by which a member of a group anonymously signs the message on behalf of the group.The server sends complaints to the Group Manager (GM) if a user misbehaves which lacks scalability. Traceable signatures traces the signatures signed by a single party without opening the signature and revealing the identities of another users. This method does not provide backward unlinkability, where the previously issued signatures remain anonymous even after the signer's revocation. Since there is no backward unlinkabilty, there will be no subjective blacklisting. Subjective blacklisting is the process by which the server can blacklist the user for whatever reason the server desires. Dynamic accumulator is cryptographic accumulator that allows dynamically adding or deleting a value. But here a single revocation operation results in a new accumulator and public parameters for the group. Thus updating all the values is impractical. In Verifier Local Revocation (VLR), [15] the verifier performs local updates but there will be heavy computation at the server or the verifier. These approaches do not provide revocation auditability by which the users can verify their status before accessing the server.

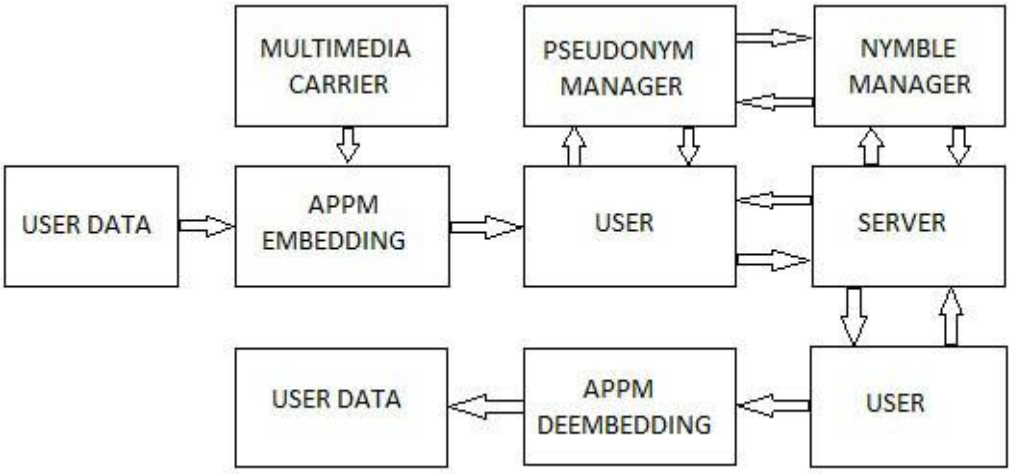
PROPOSED SYSTEM

This paper proposes a secure communication using an adaptive pixel pair matching(APPM) embedding method and nymble system. APPM is anembedding method to reduce the embedding impact by providing a modest extraction function and a more compact neighbourhood set. This embeds more messages per modification and thus increases the embedding efficiency and also brings higher payload with less detectability. After embedding data, as the information passes through several networks, to provide authentication, this paper incorporates Nymble server [2] which provides the following properties: anonymous authentication, subjective judging, fast authentication speeds, rate-limited anonymous connections, revocation auditability

Input design of the system involves the procedures for data preparation. These initial steps are necessary to put transaction data into a transformable form for processing further by the nymble system. The design of input focuses on increasing the embedding efficiency. The input to nymble system is designed in such a way that it provides security from attackers.

The information or data to be communicated is first made hidden in any multimedia carrier by the user. This is achieved by employing APPM embedding method. After embedding the data, the user establishes connection with the nymble server and transfers the embedded data via

nymble. This adds a layer of authentication to the complete system.This method can be implemented to secure any documents or files in any organisation or firms. Also documents can be shared among restricted users using nymble server. The system in which nymble system is installed acts as nymble server and can control the access of other users.



.

Fig 1:Overall system flow

ADAPTIVE PIXEL PAIR MATCHING

In ppm-based data-hiding method pixel pair $(p,q)$is used as the coordinate, and a coordinate (p',q') within the neighbourhood set $\phi(p',q')$is found such that $f(p',q')=s_B$, where f is the extraction function and s_B is the message digit in B -ary notational system to be hidden. Data embedding is done by swapping (p,q) with (p',q').For a PPM-based method, suppose a digits$_B$ is to be concealed. The range of s_B is between 0 and B-1, and a coordinate $(p',q') \varepsilon \phi(p,q)$ has to be found such that $f(p',q')= s_B$.Therefore, the range of $f(p,q)$ must be integers between 0 and B-1, and each integer must occur at least once. Further, to reduce the distortion, the number of coordinates in $\phi(p,q)$ should be as small as possible.

The finest PPM method shall satisfy the following three requirements:

1) There are exactly B coordinates in $\phi(p,q)$.

2) The values of extraction function in these coordinates are mutually exclusive.

3) The design of $f(p,q)$ and $\phi(p,q)$ should be capable of embedding digits in any notational system so that the best B can be selected to achieve lower embedding distortion [1].

Embedding Procedure

Suppose the cover image is of size $M \times M$, S is the message bits to be hidden and the size of S is mod S. First we calculate the minimum B such that all the message bits can be embedded. Then, message digits are sequentially concealed into pairs of pixels. The detailed procedure is listed as follows.

1. Find the minimum B satisfying $M \times M/2 >= S_B$ and convert S into a list of digits with a B-ary notational system S_B

2. Solve the discrete optimization problem to find c_B and $\phi_B(p,q)$.
3. In the region defined by $\phi_B(0,0)$ record the co-ordinate $(\hat{p}_i, \hat{q}_i)$ such that

$$f(\hat{p}_i, \hat{q}_i) = i,\ 0 \leq i \leq B\text{-}1$$

4. Construct a non repeat random embedding sequence Q using a key K_r
5. To embed a message digit S_B two pixels $(\hat{p}, \hat{q})$ in the cover image are selected according to the embedded sequence Q and calculate the modulus distance $d = s_B - f(p,q)$, then replace (p,q) with $(p + \hat{p}_d, q + \hat{q}_d)$.
6. Repeat Step 5 until all the message digits are embedded [1].

Extraction Procedure

To extract the embedded message digits, pixel pairs are scanned in the exact order as in the embedding procedure. The embedded message digits are the values of extraction function of the scanned pixel pairs.

1. Construct the embedding sequence Q using K_r
2. Select two pixels (p',q') sequence according to the embedded sequence Q
3. Calculate $f(p',q')$, the result is the embedded digit.
4. Repeat Steps 2 and 3 until all the message digits are extracted.
5. Finally, the message bits can be obtained by converting the extracted message digits into a binary bit stream [1].

NYMBLE SYSTEM

The anonymous networks like Tor hide a client's IP address by routing traffic through independent nodes in distinct administrative domains. However some users have misused such networks and they have frequently disfigured popular Web sites such as Wikipedia. Since administrators cannot block individual users' IP addresses, they resort to blacklisting the entire anonymizing network. Though blacklisting the entire anonymizing network can eradicate malicious activity through anonymizing networks, they also deny anonymous access to legitimate users.To crack this problem, Nymble is introduced, a system where servers blacklist misbehaving users, thus blocking users without affecting their anonymity. Nymble is thus uncertain to diverse definitions of misbehaviour. Servers can block users for any cause, and the privacy of blacklisted users is not affected

In Nymble system, nymbles are referred to as a unique type of pseudonym. To connect to Web Servers, users in the network acquire a set of nymbles. These nymbles are logically tough to link, and hence, using the collection of nymbles simulates unidentified access to services. Web sites can block users by obtaining a seed for a specific nymble, and thus allowing them to begin a connection with future nymbles from the user and those prior to the complaint remain unlinked and untraceable [2].

Thus without accessing the IP addresses of the users, servers can block anonymous users, while allowing legitimate users to connect anonymously. Nymblesystem allow the users know about their status before they are introduced to a nymble. If the users are in blacklisted status, they are disconnected immediately. A large number of anonymizing networks can rely on the

same Nymble system, and blacklisting anonymous users irrespective of their anonymizing network.

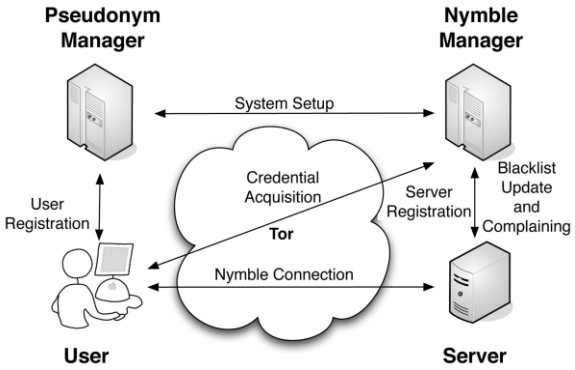


Fig 2: The Nymble system architecture showing the various modes of interaction.

The Pseudonym Manager

Initially the user must connect to Pseudonym Manager (PM) and then establish control over a resource for blocking the IP-address. The user should connect to the Pseudonym Manager directly and not through an anonymizing network, as shown in Figure 2. Pseudonym Manager has knowledge of Tor routers and can ensure that users are communicating straight with it. Pseudonyms are chosen based on the resource, which ensures that the same pseudonym is always issued for the same resource. The user does not reveal what server he wants to connect to, and the Pseudonym Manager's duties are limited to mapping IP addresses (or other resources) to pseudonyms [7].

The Nymble Manager

When the pseudonym is obtained from the PM, the user connects to the Nymble Manager (NM) through the anonymizing network, and then request for nymbles for accessing a particular server. A user's requests to the NymbleManager are therefore pseudonymous. Nymbles are generated using the user's pseudonym and the server's identity. Thereby Nymbles are specific to a particular user-server pair. As long as the Pseudonym Manager and the Nymble Manager do not collude, the Nymble Manager knows only the pseudonym-server pair, and the Pseudonym Manager knows only the user identity-pseudonym pair. To provide the required cryptographic protection and security properties, the Nymble Manager encapsulates nymbles within nymble tickets. Servers pack seeds into linking tokens [7].

RESULTS AND DISCUSSIONS

The tool used for the simulation is MATLAB version 7.10 and VB.NET. MATLAB is a high-level language and interactive environment for numerical computation, visualization, and programming.MATLAB can be used for a range of applications, including signal processing, image and video processing, control systems, test and measurement, computational finance,

Issue 3, Vol.2 (May 2013)
ISSN 2249-6149

and computational biology. To demonstrate the effectiveness of the embedding procedure, the cover image and the stego image is shown in Figure 3.

Fig 3. The cover image and the stego image

The generated stego image shows that they contain no artifacts that can be visualised by human eyes.

The screenshots of the nymble system developed using VB.NET is shown in Figure 4.

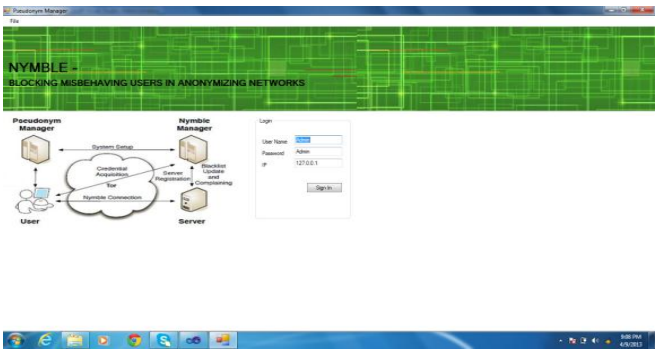


Fig 4 (a): Connecting to PM

Fig 4 (b): Connecting to NM

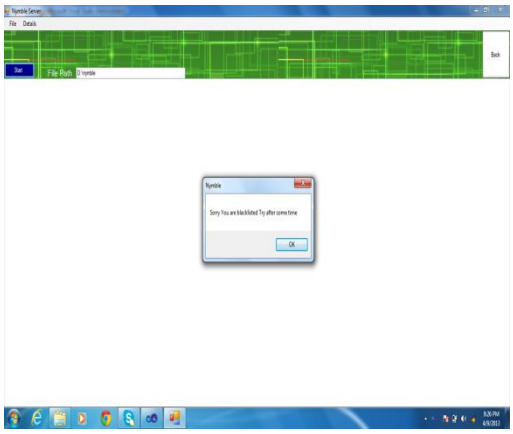


Fig 4 (c): Denying the misbehaving user

CONCLUSION

This paper proposes a secure communication for users with the help of Nymble server and Adaptive pixel pair matching embedding method.Different steganographic scheme has been discussed in the part of literature survey with its pros and cons. Different applications require different steganographic schemes, with different strong and weak points.This adaptive steganography is not an easy target for attackers, especially when the hidden information is small. This method tends to have higher payload when compared with other steganographic technique.After embedding, the image file is saved in memory from where users access is restricted using nymble server. Thus important documents or files in any organisation can be secured well by implementing the proposed system.

ACKNOWLEDGMENTS

The authors would like to thank each and every one, who did timely helps and gave valuable suggestions during the period of this work which have helped to improve the quality of this paper.

REFERENCE

[1]Wien Hong and Tung-Shou Chen , “A Novel Data Embedding Method Using Adaptive Pixel Pair Matching,” IEEE Transactions On Information Forensics And Security, Vol. 7, No. 1, February,2012.

[2] Patrick P. Tsang, ApuKapadia, “Nymble: Blocking Misbehaving Users in Anonymizing Networks,” IEEE Transactions On Dependable And Secure Computing, VOL. 8, NO. 2, March-April,2011.

[3] Provos.N and Honeyman.P, “Hide and seek: An introduction to steganography,” IEEE Security Privacy, vol. 3, no. 3, pp. 32–44, May/Jun,2003.

[4] Wien Honga, Tung-ShouChenb, Chih-Wei Luoa, "Data embedding using pixel value differencing and diamond encoding with multiple-base notational system," The Journal of Systems and Software 85 , 1166– 1175,2012.

[5] J. Wang, Y. Sun, H. Xu, K. Chen, H. J. Kim, and S. H. Joo, "An improved section-wise exploiting modification direction method," Signal Process., vol. 90, no. 11, pp. 2954–2964, 2010.

[6] Wu D.C., Tsai W.H, "A steganographic method for images by pixel-value differencing," Pattern Recognition Letters 24, 1613–1626,2003.

[7] P.C. Johnson, A. Kapadia, P.P. Tsang, and S.W. Smith, "Nymble: Anonymous IP-Address Blocking," Proc. Conf. Privacy Enhancing Technologies, Springer, pp. 113-133, 2007.

[8] C. K. Chan and L. M. Cheng, "Hiding data in images by simple LSB substitution," Pattern Recognit., vol. 37, no. 3, pp. 469–474, 2004.

[9] J. Mielikainen, "LSB matching revisited," IEEE Signal Process. Lett., vol. 13, no. 5, pp. 285–287, May 2006.

[10] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," IEEE Commun.Lett., vol. 10, no. 11, pp. 781–783, Nov. 2006.

[11] Cheddad A, Condell J, Curran K, and McKevittP , "Digital image steganography: Survey and analysis of current methods," Signal Process., vol. 90, pp. 727–752,2010.

[12] R.M. Chao, H. C. Wu, C. C. Lee, and Y. P. Chu, "A novel image data hiding scheme with diamond encoding," EURASIP J. Inf. Security, vol. 2009, 2009, DOI: 10.1155/2009/658047, Article ID 658047.

[13] Kim H.J, Kim C, Choi Y,. Wang S, X. Zhang, "Improved modification direction methods," Computers and Mathematics with Applications 60,319_325,2010.

[14] G. Ateniese, D.X. Song, and G. Tsudik, ―Group Signatures, Proc. Conf. Financial Cryptography, Springer, pp. 183-197, 2010.

[15] P.P. Tsang, M.H. Au, A. Kapadia, and S.W. Smith, ―PEREA: Towards Practical TTP-Free Revocation in Anonymous Authentication, Proc. ACM Conf. Computer and Comm. Security, pp. 333-344, 2008.