Journal of Management and Social Studies

Volume 2, Issue 2, February 2024, pp. 22-33

Copyright© 2023, CSTIJ Publication

homepages: http://cstij.org/

Develop Information Security based on Steganographic Model

Saleem Issa Al-zoubi[1*]

[1] Faculty of Information Technology, Irbid National University

*Corresponding author's E-mail: *it@inu.edu.jo*

ABSTRACT

As a result of the carried out analysis of existing methods Steganography of protection of the information their lacks are certain, the ways of their elimination are produced by updating the known DES-standard and development of an original method of protection of the password from breakings and disclosure. The algorithm of formation of a key sequence is developed which automatically each day changes at the constant password. It appreciably simplifies procedure of change of the passwords and their preservation. Use of the individual additive makes to more safe disclosure of the user password. Due to this the breaking of the password becomes practically impossible.

Keywords: Steganographic model, password, Information Security, Secret Key.

1. Introduction

In recent years, the problems associated with information protection, attracting increasing attention as a specialist in computer security, as well as many casual users of computer systems. This is due to the profound changes introduced by computer technology in your life.

It changed the whole approach to the concept of "information". This term is often used to refer to a special product that you can buy, sell, trade it for something else, etc. The cost of such a product often exceeds tens or even hundreds of times the cost of the computer system within which it operates.

Naturally, there is a need to protect information from unauthorized access, theft, destruction, and other criminal activities. Separately, there is a question of copyright protection for information products: software, algorithms, data, results [4].

Message that someone can steal information that is processed in a computer network, now very few people will be surprised. Methods of entry into the network and the subsequent theft of information are well known. The most effective is the implementation of the system software - the bookmark. Depending on the goals the program - the tab can, for example, to intercept passwords or specific criteria to find the information on hard drives. In the future, the collected information is sent via e-mail address to a pre-conditioned. Accordingly, all system administrators are taking some measures to prevent such attempts. This makes the hackers invent new methods of entry into the network or to improve the well-known [8].

There are two of the most difficult for the attacker's point: installing a program - a bookmark ("Trojan horse") and explored the transfer of information. In these moments of intelligence activity the easiest to detect. Moreover, the greater the volume of the program being implemented or the amount of transmitted data such program, the greater the likelihood that intelligence activities will be detected and stopped. The need to conceal the transfer of the message inevitably leads to the introduction of malicious methods of Steganography (covert data) [2].

How many of mankind, so there is a problem of information exchange. On the one hand, people tend to communicate and exchange information with each other, on the other hand tend to hide from strangers are not only information but also the fact of its transmission. Therefore, humanity is rapidly developing as a means of transmission and means of hiding information. For information hiding techniques applied cryptography and Steganography . Cryptography - a system of changing the information in order to make it unintelligible to the uninitiated persons. Steganography - a system of changing the information in order to hide the very existence of the secret message.

The word "Steganography " is derived from the Greek words "steganos" - the secret and "graphy" - record and literally means "secret writing". Unlike cryptography, where an outside observer can easily determine the transfer of an encrypted message, the methods of Steganography conceal the very fact of transfer secret information, and for improving its protection against opening the secret information can be additionally encrypted [1].

You will notice an important distinguishing feature of Steganography (which we need in the future): Methods of Steganography have suggested that the fact that some exchange of information is not hidden. However, it is assumed that the transmitted message will looks kind of censor. Therefore, under the concealment of the transfer of information in Steganography is understood not only (perhaps not so much) that referred to the censor cann't find what you are viewing a message, there is another (hidden) message, but the fact that the transmitted message should not cause the censor suspicion. If you suspect a trick the censor, it just overrides the channel of information transfer.

Despite such rapid development of Steganography techniques to protect confidential information in this area of research and practical developments there are many unsolved problems [6].

Thus, the requirements of reliability to hide sensitive information, reduce the impact of interference on the transmitted encrypted message with a simultaneous decrease in the cost of the protection system as a whole led to the relevance, purpose and objectives of the research [5].

2. Literature Review

2.1. Overview of the known methods Steganographic.

Steganography is a process that involves hiding a message in an appropriate carrier like image or audio. It is of Greek origin and means "Covered or hidden writing". The carrier can be sent to a receiver without anyone except the authenticated receiver only knows existence of the information. Steganography is an emerging area which is used for secured data transmission over any public media. Considerable amount of work has been carried out by different researchers on steganography.

Currently, methods of computer Steganography developed in two main areas:

1. Methods based on the use of special properties of computer formats;
2. Methods based on the redundancy of the audio and visual information.

Methods of using the redundancy of digital photography, digital audio and digital video Low level of digital samples contain very little useful information. They filled more information does not affect the quality of experience that allows you to hide sensitive information by introducing additional information distorted the statistical characteristics of digital streams. To reduce the signs of compromise requires correction of statistical characteristics of the latent ability to transfer large amounts of information.

The possibility of copyright protection, the latent image of the brand, registration numbers, etc [10].

The first direction based on the use of special properties of computer data formats, and not on the redundancy of the data. Special properties of selected formats, taking into account protection of concealed messages from direct listening, viewing or reading. Based on the analysis of the data table. One can conclude that the main direction of computer Steganography is the use of redundant audio and visual information. Digital photography, digital music, digital video - numbers are represented by matrices that encode the intensity at discrete points in space and / or time. Digital Photography - a matrix of numbers representing the intensity of light at a certain

time. Digital audio - it is a matrix of numbers representing the intensity of the sound signal in consecutive moments of time. All these numbers are not exact, since devices are not accurate digitizing of analog signals, there is quantization noise. Junior level digital samples contain very little useful information about the current parameters of the sound and visual images. They are filling does not affect significantly the quality of perception that allows to hide the additional information [9].

Graphics files with a scheme color mixing RGB code for each point of the figure three bytes. Each point consists of the additive components: red, green and blue. Change each of the three least significant bits leads to a change of less than 1% of the intensity of a given point. It hides the standard graphical image of 800 Kbytes 100 Kbytes of information that is not noticeable when viewing images.

Another example. Only one second of digital audio with a frequency of 44100 Hz and 8 bits of the reference level in the stereo mode allows you to hide by replacing the least significant bits in the lower concealed message about 10 Kbytes of information. The change in value of samples is less than 1%. This change in practice can't be detected when listening to the file, the majority of people [7].

2.2. Development of a method of forming the password

A very sensitive place any system cryptography with the private key is to know the password to all users. In this case, the possibility of uncontrolled leakage of information about the structure of the password. It is therefore necessary to take additional measures for the preservation of privacy password.

To solve this problem will detail the concept of a password. Consider the following passwords:

• The system password.
• The user's password.
• An individual password.

Traditional systems cryptography treat all three as a single password. If they are to separate, we can achieve some positive moments. System Password - this is a secret sequence of characters, which is formed by a key sequence. It is not known to any user. User password - it is a secret sequence of characters, from which later formed the system password. The user password known the full range of registered users. The longer the password, the more priority access to the information the user has.

Individual password - this is a secret, individual for each user, a sequence of characters that identifies him personally. A feature of this password is what it is for different users different (2-16 bytes).

Also, we introduce a password as a key administrator. This so-called server password. It is needed to ensure that each user has access to information from only one of the server, that is from a different server computers access to the information it will be closed.

A system password is obtained by transforming the key administrator, user, individual passwords and specific supplements for each individual user. This additive is formed when a user logs in such a way that it, together with a key administrator, standard user passwords and individual

giving the system password. This addition is written to the server.The structure of the procedure of forming the system password shown in fig.3.1.

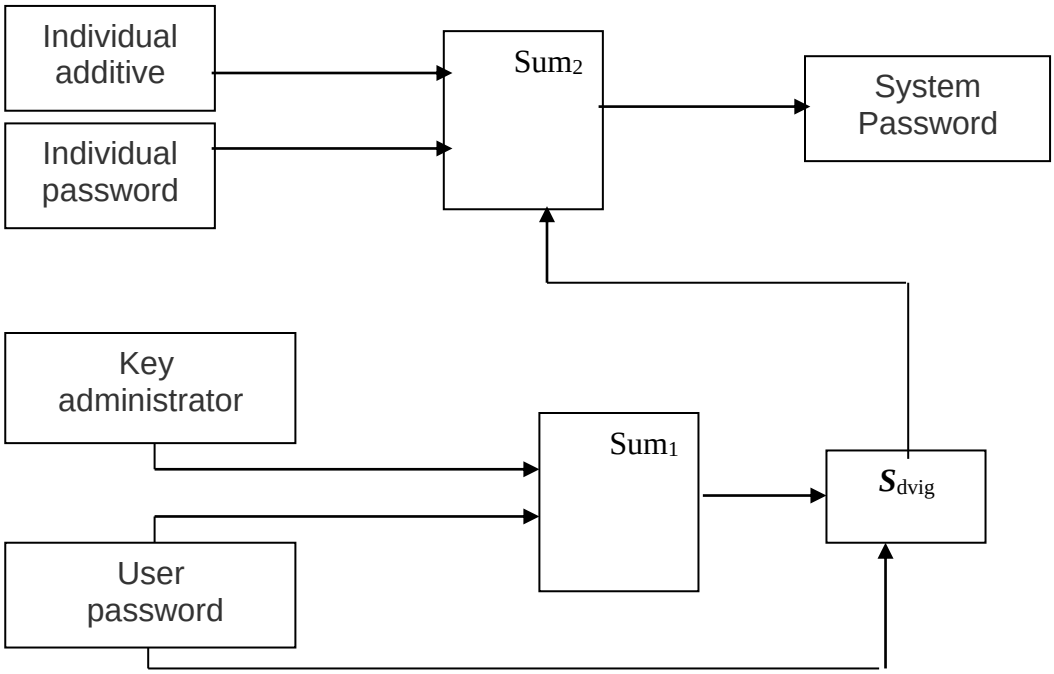
Figure 1 The procedure of forming the system password

3.1 Development of the algorithm of formation of key.

Cryptographic protection of binary information carried by transforming the original (open) the text in the encrypted message to a well-known algorithm by using the secret key sequence. The maximum password length can be 32 bytes = 256 bits, which gives the number of possible passwords 2256, which significantly outperforms all known methods. A key sequence, respectively, is a procedural molded 256-mi bit code based on a 32-byte password (known to a limited circle of people) and the aggregate value of the month and day of week. Background to the formation of a key sequence is entered in a removable ROM (for software implementation - randomly generated in a specific area of RAM).

The peculiarity of the functions of key generation is the possibility of unauthorized receipt only if the knowledge:

- Individual passwords.
- User's password.
- Key diskette.
- Algorithm for formation of the key.



- The contents of the secret ROM.

The absence of even one of the components making it virtually impossible to process selection key attacker. Key generation algorithm is as follows. The number (s) of the month and day (d) are the initial weeks of information to determine the start of a binary sequence, which forms a key. Number of primary sequence of bits is defined as

n = 8 * c + d. nmax = 8 * 31 = 255 7.

Sequence length N = 512 bits. The limit capacity of the ROM is:
E = nmax + N = 255 + 1024 = 1279 bits.
The procedure for generating the key from the selected sequence has the form shown in Fig.3.2.

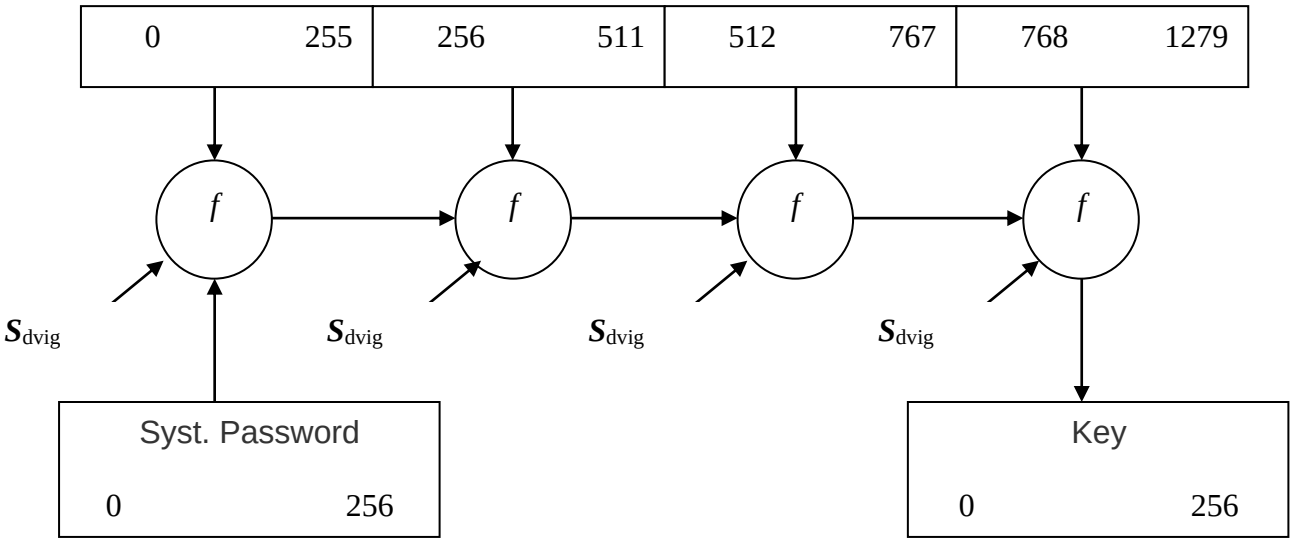


Figure 2: The procedure for the formation of key

Since the procedure is irreversible key generation, the role of the function f may make any bitwise logical operations. However, it should be noted that the logical multiplication will give the dominance of zeros in the key sequence, and the logical disjunction - the dominance of units, which is not desirable, because it dramatically reduces the number of keys with a large number of passwords. From this point of view of "neutral" logical operation is the sum modulo two. The algorithm cryptography constructed in such a way that to encrypt a portion of the eight input bytes necessary to carry out eight iterations with selecting the number of 32-bit sequences of the 256-bit sequence KEY. Moreover, depending on the priority of access to classified information, the value of parolevoy PAROL sequences can vary from 4 to 32 bytes. The shorter the password, the more areas of overlap in the 32-digit key generated sequences.
These address the initial sample stored in ROM (for hardware implementation) or generated in the RAM (for program implementation). Number of characters of the password is determined by its effect through the introduction and K. Sign in cryptography to encrypt or decrypt the information is possible only if the following requirements:
- If its registered key diskette;
- With the right administration of individual password.
After a successful login you can get access right to authorized user documents. The right of access is determined by comparing the number of characters entered with a valid user password for a particular user the size of the user password recorded on the individual key diskette.
The proposed procedure for protection of key sequences from the selection automatically changes it once at the beginning of the day. Therefore, one disadvantage of this method is the strict observance of the conditions and encryption and decryption for one day. However, this observation applies only to the operational cryptography for transmission on the network. When decrypting files that are stored background information for the key sequence does not favor the

current date and closing date of the file.

The developed algorithm for the formation of a key sequence that automatically changes every day with unchanged passwords. This greatly simplifies the process of changing passwords and save them. Using a floppy disk with the addition of the individual making the disclosure of a more secure user passwords. The use of an additional question from the questionnaire by making it virtually impossible to access information by unauthorized persons.

3. Methodology

The proposed algorithm is based on the well-studied DES-method. His modification consists of the following:

- May be flexibly resizable parolevoy sequence of 4 bytes to 32;
- Lack of input and output permutations of characters encoded in a series;
- Use to encrypt information on the status symbol in the outbound document;
- Increased the size of the encoded portion of up to 8 bytes.

The procedure cryptography iterative and consists of a reversible bitwise logical operations, permutations and cyclic shifts left (L) and right (R) of two bytes and is presented in ris.3.3. cryptography function F is the sum modulo 2 of the i-th part of the key Ki, the right side of the encoded portion of Ri-1 and the function of Pol followed by a cyclic shift to the left. Some of the key is taken from the table. 3.1, depending on the number of iterations and the size of parolevoy sequence. The argument specifies the number of digits Pol Ri-1, in which additional units are added, depending on the atomic number kriptiruemoy eight bytes. The number of shifts to the left must be a multiple of two, and the same for all iterations of the loop cryptography one of four characters. It is determined by the code, obtained from 0.16 and 31 bits of a key sequence, multiplied by 2.

For example, if you received the following key sequence:

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
1	0	0	1	1	1	0	0	1	1	1	1	0	0	1	0	0	1	0	1	1	1	0	1	1	1	1	0	0	0	0	1

Then the number of shifts will be as follows (101) 2 * 2 = (5) 10 * 2 = 10.

Length. password / № iteration	1	2	3	4	5	6	7	8
4	0	0	0	0	0	0	0	0
5	0	2	3	4	5	6	7	8
6	0	4	6	8	10	12	14	16
7	0	6	9	12	15	18	21	24
8	0	2	7	12	17	22	27	32
9	0	4	10	16	22	28	34	40
10	0	6	13	20	27	34	41	48
11	0	8	16	24	32	40	48	56
12	0	10	19	28	37	46	55	64
13	0	12	22	32	42	52	62	72
14	0	14	25	36	47	58	69	80
15	0	16	28	40	52	64	76	88
16	0	18	31	44	57	70	83	96
17	0	20	34	48	62	76	90	104
18	0	22	37	52	67	82	97	112
19	0	24	40	56	72	88	104	120
20	0	26	43	60	77	94	111	128
21	0	28	46	64	82	100	118	136
22	0	30	49	68	87	106	125	144
23	0	32	52	72	92	112	132	152
24	0	34	55	76	97	118	139	160
25	0	36	58	80	102	124	146	168
26	0	38	61	84	107	130	153	176
27	0	40	64	88	112	136	160	184
28	0	42	67	92	117	142	167	192
29	0	44	70	96	122	148	174	200
30	0	46	73	100	127	154	181	208
31	0	48	76	104	132	160	188	216
32	0	32	64	96	128	160	192	224

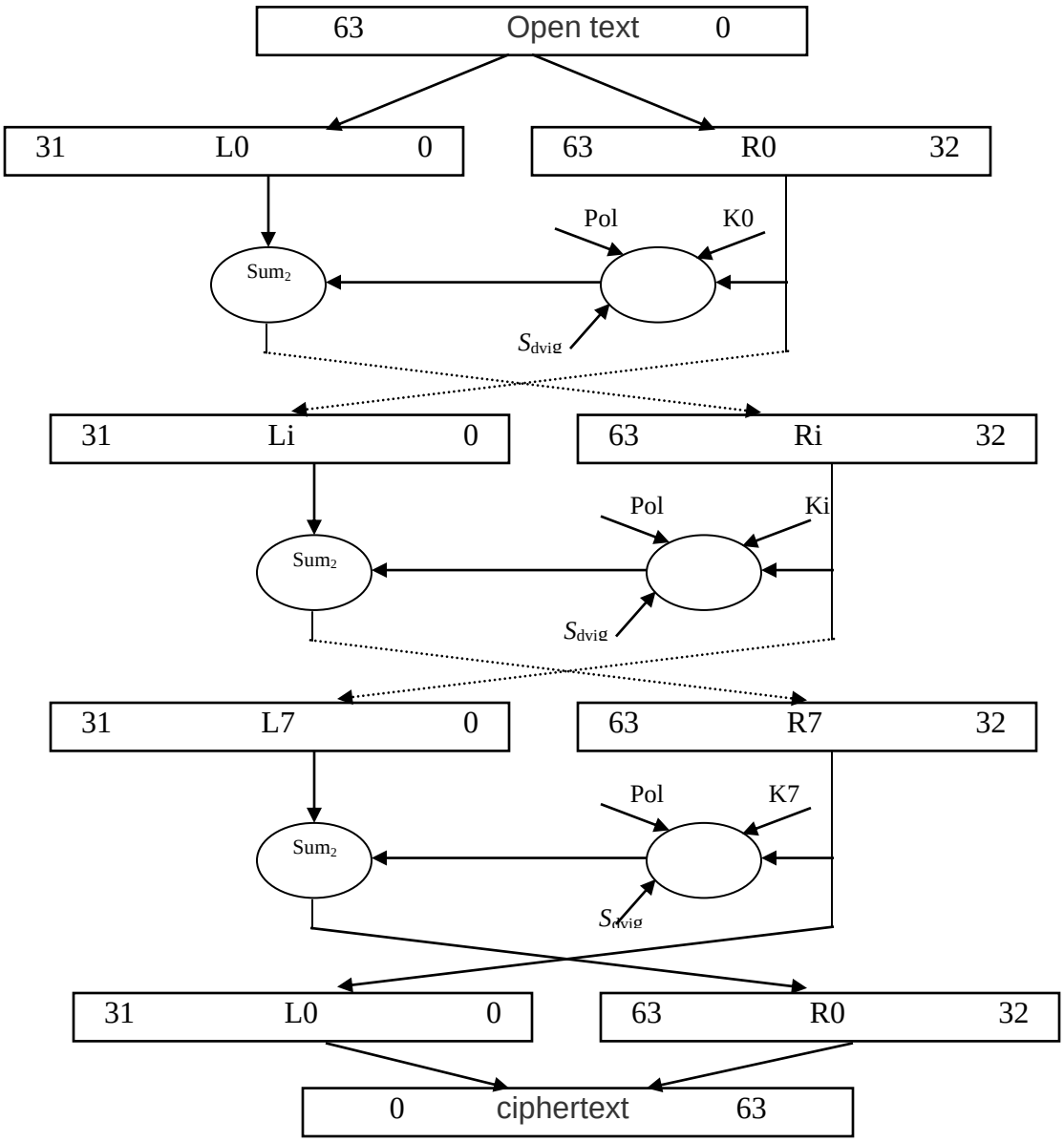


Fig. 3 Structure of the proposed method of encryption

4. Finding

This model is reduce the impact of interference on the transmitted encrypted message with a simultaneous decrease in the cost of the protection system as a whole led to the relevance it easily as shown in fig.1.4

Empty Container: 210 KB file format *. Bmp

The filled container: 210 KB file format *. Bmp

Hidden file size 40 KB format *. Doc

(a) (b)

In Fig. 4 Example images of empty (a) and filled (b) containers

5. Discussion & Conclusion

The analysis of existing methods of Steganography protect information defined by their flaws, worked out ways to eliminate them by modifying the well-known DES-standard and develop an original method of password protection against hacking and disclosure.

An algorithm for the formation of a key sequence that automatically changes every day at a fixed password. This greatly simplifies the process of changing passwords and save them. The use of individual supplements the disclosure makes it more secure user passwords. With this hack password becomes almost impossible.

A successful modification of the standard DES-authorized for encryption and decryption use the same algorithm, which greatly simplifies the hardware implementation.

References:

1. S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain. A New Approach for LSB Based Image Steganography using Secret Key, 987-161284-908-9/11/$26.00, 2011 IEEE.
2. T Mrkel,JHP Eloff and MS Olivier .”An Overview of Image Steganography,”in proceedings of the fifth annual Information Security South Africa Conference ,2005.
3. “An Image based Steganography model for promoting Global Cyber Security” by Souvik Bhattacharyya , Gautam Sanyal and Arka Majumdar at the proceedings of “International Conference on Systemics,Cybernetics and Informatics (ICSCI-2009)”
4. “Implementation and Design of an Image based Steganographic model” by Souvik Bhattacharyya and Gautam Sanyal at the proceedings of “ IEEE International Advance Computing Conference “(IACC-2009)”.
5. M. Hossain, S.A. Haque, F. Sharmin, "Variable Rate Steganography in Gray Scale Digital Images UsingNeighborhood Pixel Iriformation", Proceedings of 2009 12th International Conference on Computer and Information Technology (ICCIT 2009) 21-23 December 2009, Dhaka, Bangladesh.
6. N.F. Johnson, S. Jajodia. Exploring Steganography: Seeing the Unseen, IEEE Computer, February 1998, vol. 31, no. 2, pp.26-34.
7. Walter Bender, Daniel Gruhl, Norishige Morimoto, and Anthony Lu. Techniques for data hiding. IBM Systems Journal, 35(3 & 4):313{336, 1996.
8. Raymond B. Wolfgang and Edward J. Delp. A watermark for digital images. In International Conference on Images Processing, pages 219-222, Lausanne, Switzerland, September 1996. IEEE.
9. Nicholas Hopper, Luis von Ahn, and John Langford. Provably Secure Steganography, IEEE TRANSACTIONS ON COMPUTERS, VOL. 58, NO. 5, MAY 2009.
10. HAO-BIN, ZHAO LI-YI, ZHONG Wei-Dong. A Novel Steganography Algorithm Based on Motion Vector and Matrix Encoding, 978-1-61284-486-2/11/$26.00 ©2011 IEEE.