Information Hiding Using E-mail Cards

Dr. Abdul Monem S. Rahma *
Computer Science Depart.
University of Technology
Baghdad, Iraq
monemrahma@yahoo.com

Hend Abdul Rezaak Khalaf **
Computer Science Depart.
University of Technology

Abstract:

Steganography, is the hiding and transmitting secret messages through apparently innocuous carriers in an effort to conceal the existence of them. The carrier can be anthing used to transfer information, including, e-mail, audio, video, images, messages, disk partitions and disk space.
The aim of the research is for hiding a text message in the unused spaces of the e-mail card structure which is designed by Macromedia Flash software (SWF file).
Macromedia Flash (SWF (Shockwave File) file) has been chosen because as it is widely used in Internet (Web pages), is recognized by all browsers and it is easily distributable which ensures that it lends itself to this type of activity without drawing attention to itself.
The research studies different types of e-mail cards and show the possibility of them to hide secret message.

The research deduces that the e-mail card which is designed from sound, animation and moving image is good for hiding (because it contains many unused spaces available for hiding).

الاخفاء المعلوماتي باستخدام البطاقات البريدية

د.عبد المنعم صالح ابو طبيخ *
الجامعه التكنولوجيه
قسم علم الحاسبات

هند عبد الرزاق خلف **
الجامعه لتكنولوجيه
قسم علم الحاسبات

الملخص:

علم الاخفاء (steganography) هو أخفاء ونقل الرسائل السرية (secret messages) خلال ناقل غير مثير للشكوك ظاهريا (innocuous carrier) في محاولة لاخفاء وجودهم. والناقل (carrier) يمكن ان يكون اي شيء يستخدم لنقل المعلومات، يتضمن، البريد الالكتروني(e-mail)، صوت (audio)، فيديو (video)، صور (images)، رسائل (messages)، اقسام الدسك (disk partitions) و فراغات الدسك (disk spaces).

هدف البحث هو اخفاء رسالة نصية (text message) في الاماكن الغير مستخدمة (unused spaces) لهيكلية بطاقة البريد الالكتروني (e-mail cards) المصممة باستخدام Macromedia Flash Software (SWF file) ، وذلك لكثرة استخدامه في الانترنت وخاصة في صفحات الويب (Web pages)، وهو معروف من قبل برامج تصفح الانترنت (browsers)، وسهولة انتشاره تؤكد فعاليته بدون جلب الانتباه اليه.

درس البحث العديد من البطاقات البريدية وبين مدى امكانيتها لاخفاء الرسائل النصية. استنتج البحث ان البطاقة البريدية المصممة من صوت (audio)، صورة متحركة (moving image)، وحركة (animation) تعتبر بطاقة جيدة للاخفاء لانها تحتوي العديد من الفراغات الغير مستخدمة (unused spaces).

---

* الجامعة التكنولوجية – قسم علوم الحاسبات.
** الجامعة التكنولوجية – قسم علوم الحاسبات.

1. Introduction:

Information hiding techniques have recently become important in a number of application areas. Digital audio, video, and pictures are increasingly furnished with distinguishing but imperceptible marks, which may contain a hidden copyright notice or serial number or even help to prevent unauthorized copying directly [1].

Steganography (the art and science of hiding information by embedding messages within other, seemingly harmless carriers) destined to become more important as more people join the Cyberspace revolution and as the existing governments of the world attempt to regulate or prohibit the use of cryptography for personal privacy purposes. If the government prohibits the use of cryptography, a person can still send encrypted messages by hiding the encrypted message in another innocuous file using steganographic techniques. And thus another attempt to control Cyberspace can be thwarted by technology [2].

Typically, stego utilities protect data by firstly, hiding its existence, and secondly, encrypting the hidden data, so that even if the object is discovered it still has to be decrypted. Good stego applications will not allow the user to embed a message in an unsuitable carrier, and allow for a variety of algorithms (each with distinctive characteristics) [3].

Steganography works by replacing bits of useless or unused data in regular computer files (such as graphics, sound, text, HTML, or even floppy disks) with bits of different, invisible information. This hidden information can be plain text, cipher text, or even images [4].

Obviously, the explosion of Internet traffic provides the perfect environment for data hiding via steganography. With the vast amount of potential cover files that are posted, e-mailed, and viewed on Web pages every day, it is impossible to manually scan even a fraction of them. Tremendous potential exists for a significant amount of illicit traffic to go undetected by law enforcement. Furthermore, as the bandwidth of the Internet increases to afford easier transmission of large files such a real time video, there will be an increased risk that illegal communications will go undetected [5]. Figure (1) shows the general model of hiding a message in e-mail card.

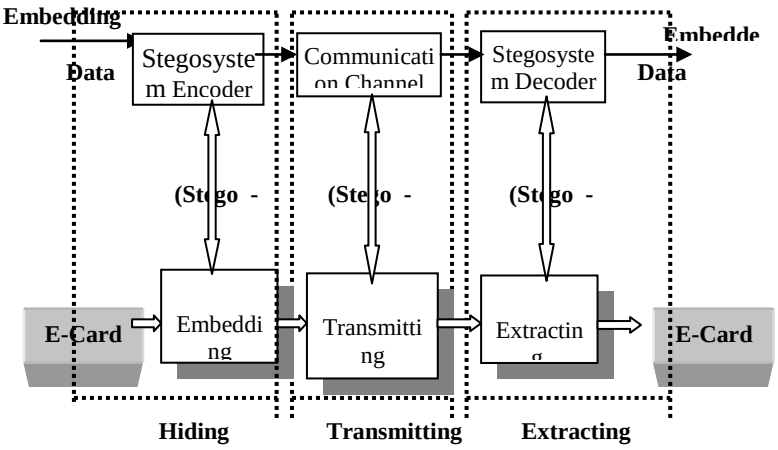

Figure (1) General Model of Hiding a Message in E-Cards

2. E-mail Card overview:

E-mail cards currently represent the second highest activity on the Web behind e-mail. The uses of e-mail cards are the perfect way to delivery person's customized holiday or special occasion greeting via email and the person can get rid from the hassle and expense of mailing cards when he or she can send them instantly via e-mail [6].

Sending an electronic greeting card is a fun, effective and popular way to stay in touch

with friends and family. The person can use his or her own photo on an e-mail card or choose from the many photos such as holidays, special occasions, birthdays, and subjects such as love or congratulations and sends it to many persons at the same time. Also e-mail cards are a proven success; they are a great way for businesses to build relationships with their clients. Or for individuals to get quality return visitors to their sites and make money from advertising or sales of products [7].

Usually the ecards are used to:

- promote - promote products and services.
- brand - create company awareness among businessman client base.
- invite - invite people to seminars and special events.
- remind - send appointment reminders.
- inform - send Client appreciation memos, Recruiting/hiring notices, etc.
- reference - send Birthday wishes, Holiday greetings, Thank You's, etc.

Although there exist many different software types for designing the e-mail cards, such as: Corel Draw, Adobe Photoshop and Macromedia Flash, the Macromedia Flash software is chosen for designing the e-mail cards, since Macromedia Flash contains many flexible features which will be discussed later.

3. Design E-mail Cards Using Macromedia Flash Software:

Macromedia Flash is a popular program used by Web designers to create exciting, interactive, dynamic and attractive, Websites, e-mail cards with anti-aliased graphics and animations. Flash is the technology known to support sites with vector, bitmap graphics, mp3 (**M**PEG **P**layer 3) sound, interactivity, games, animation motion and much more With flash, Web designers can creates professional standard graphics using the normal drawing tools and apply motion to create a short animation to import onto Websites [8].

Flash is stored in highly compressed binary files known as SWF (pronounced ‘Swiff’) files which is a completed compression version of the flash file that is viewable on the Internet [9].

The Macromedia Flash (SWF) file format was designed to deliver vector graphics and animation over the Internet, it's a very efficient delivery format and not as a format for exchanging graphics between graphics editors.

SWF was designed to meet the following goals:

- **On-screen Display**—The format is primarily intended for on-screen display and so it supports anti-aliasing, fast rendering to a bitmap of any color format, animation and interactive buttons.
- **Network Delivery**—The files can be delivered over a network with limited and unpredictable bandwidth. The files are compressed to be small and support incremental rendering through streaming. SWF is a binary format and is not human readable like HTML. Macromedia Flash (SWF) uses techniques such as bit-packing and structures with optional fields, to minimize file size.
- **Simplicity**—The format is simple so that the player is small and easily ported. Also, the player depends upon only a very limited set of operating system functionality.
- **Speed**—The files are designed to be rendered at a high quality very quickly.

- **Extensibility**—The format is a tagged format, so the format can be evolved with new features while maintaining backward compatibility with older players.
- **Scalability**—Different computers have different monitors resolutions and bit depths. Files work well on limited hardware, while taking advantage of more expensive hardware when it is available.
- **File Independence**—Files can be displayed without any dependence on external resources such as fonts.

4. E-mail Card Structure: [10]

The format of the e-mail card structure (SWF file) has two main components – the headers and the frames. The headers store information such as the size of the movie, the version, how many frames it has, its size and the frame rate. All Macromedia Flash (SWF) files begin with the header as shown in table (1).

Table (1): E-mail card (SWF) File Header

SWF File Header		
Field	**Type**	**Comment**
Signature	UI8	Signature byte always 'F'
Signature	UI8	Signature byte always 'W'
Signature	UI8	Signature byte always 'S'
Version	UI8	Single byte file version (e.g. 0x04F for SWF 4)
File Length	UI32	Length of entire file in bytes
Frame Size	RECT	Frame size in twips
Frame Rate	UI16	Frame delay in 8.8 fixed number of frames per second
Frame Count	UI16	Total number of frames in movie

The header beings with the three-byte **Signature** 0x46, 0x57, 0x53 ("FWS") followed by a one-byte **Version** number. The version number is not an ASCII character, but an 8-bit number. For example, for SWF 4 the version byte is 0x04, not the ASCII character '4' (0x35).The **File Length** field is the total length of the SWF file including the header. The **Frame Size** field defines the width and height of the movie. This is stored as a RECT structure. The **Frame Rate** is the desired playback rate in frames per second. This rate is not guaranteed if the SWF file contains streaming sound data, or the player is running on a slow CPU. The **Frame Count** is the total number of frames in this SWF movie.

Following the header are a series of tagged data blocks as shown in figure (2).

Figure (2) E-mail card (SWF) File Structure

All tags share a common format, so any program parsing a Macromedia Flash (SWF) file can skip over blocks it does not understand. Data inside the block can point to offsets within the block, but can never point to an offset in another block. This enables tags to be removed, inserted, or modified by tools that process a SWF file. There are two categories of tag in Macromedia Flash (SWF):

Definition tags define objects such as shapes, buttons, sprites (embedded Flash movies), text, sound and embedded images. These can be thought of as the actors in a movie.

Control tags control the flow of the movie. They are responsible for placing, modifying and removing the actors from the screen. Control tags

can be divided into three categories: display list, control, and action as shown in figure (3).

Display List tags	Control tags	Action tags
PlaceObject	End	
PlaceObject2	Protect	DoAction
RemoveObject	FrameLabel	
RemoveObject2	SetBackgroundColor	
ShowFrame	StartSound	

Figure (3) Categories of Control Tags

Every definition tag must specify a unique ID. Duplicate IDs are not allowed. Typically, the first CharacterId is 1; the second CharacterId is 2 and so on. Character zero is special and considered a null character. Control tags are not the only tags that reference the dictionary. Definition tags can use characters from the dictionary to define more complex objects. For example, the DefineButton tag refers to characters to define the four states of the button. The DefineText tag can refer to a font character to select different fonts in the text. The diagram in figure (4) illustrates the interaction between definition tags, control tags and the dictionary.

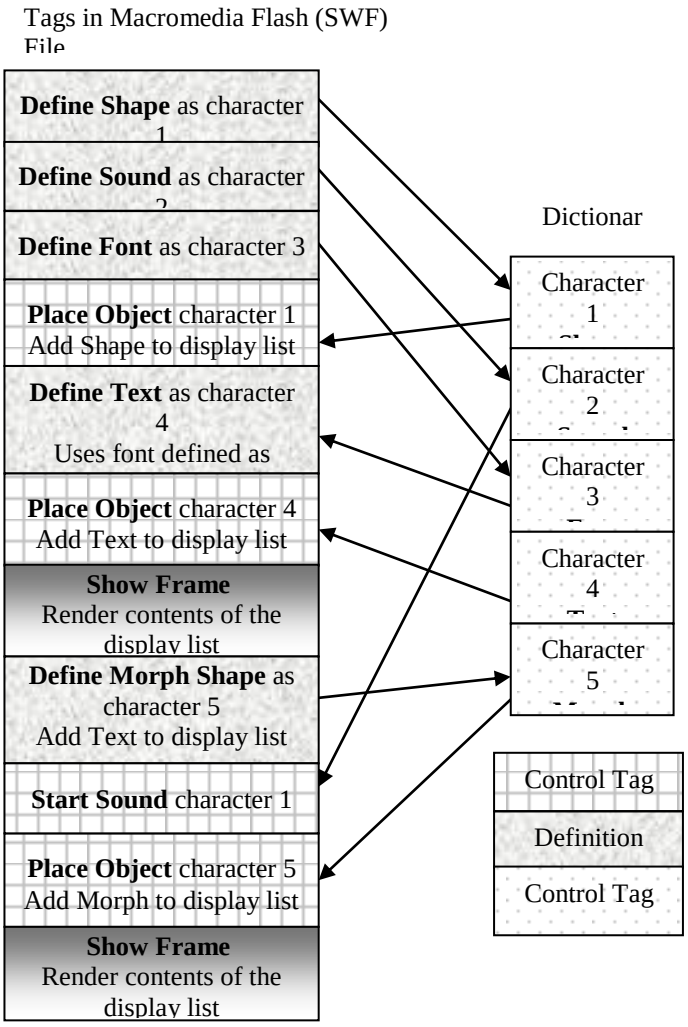

Figure (4) Interaction between Definition Tags, Control Tags and the Dictionary

5. Hiding Technique:

The hiding technique begins by searching operation in e-mail card structure for (suitable places) unused spaces and then using these spaces to hide a message after encrypting it by applying RSA encryption (with / without using password), otherwise RSA encryption and XOR encryption will be applied respectively (in case of using password).

5.1. Searching for Unused Spaces in E-mail Card Structure:

As the e-mail card structure and its header have become known, the first stage in the hiding process is to search for unused spaces in

the e-mail card structure which is done automatically in the proposed system after selecting the e-mail card from directory. The process begins by reading the header of the e-mail card (SWF file), excludes it and finds the lookup table of the e-mail card structure. The lookup table contains all the branches (conditional, unconditional), all tags addresses that are linked to it like (Sound, Image, Text, etc...), beginning and ending positions of the unused spaces between tags.

After that the searching begins by checking one byte at a time if it is related to conditional or unconditional branch, if it is, the search operation will ignore it and take the next byte and checks it, if it is free the proposed system will put it into an array in the memory for further use, this operation is done until reaching the end of the e-mail card structure.

After gathering all the unused spaces in the e-mail card as an array, another checking is done by taking one block at a time. If it contains only one or a sequence of two unused spaces, it will be ignored, except the blocks which contain more than two spaces in sequence will be used in the hiding process, because two spaces of them will be used as an index for the hidden message in cases of extracting or searching.

The Searching for Unused Spaces in E-mail Card Structure algorithm is shown below:

Input: E-mail card

Output: Total unused spaces available for Hiding

Step 1: Open the e-mail card structure (SWF file) in binary mode.

Step 2: Read the header of the SWF file and exclude it from searching.

Step 3: Read one byte.

Step 4: If byte value = 0 or byte value = 255 then
If this byte is not in lookup table then add it to an array
Else skip it.

Step 5: Loop to step 3 until reaching to the end of the SWF file.

Step 6: Close the SWF file.

Step 7: open the array, If the spaces are not beside each other then skip these spaces and remove them from the array
Else
If the spaces are beside each other & equal to or greater than 3 spaces then put these spaces into a block for further use.
Else
Skip them (spaces are less than 3 spaces).
End If
End If

Step 8: Put indexes for each block of spaces to recognize it in the proposed system as the beginning and ending of each block in case of searching for a hidden message & extraction it.

Step 9: Stop.

5.2. Hiding Process:

From the previous section the suitable place (unused space) is found which limits the number of characters. It is possible to hide a message in the e-mail card structure. For example, the greeting e-mail card (which was designed from animation, sound, animated text, and image) as shown in figure (5) is chosen to hide a message in it.

Figure (5) An example of Flash greeting e-mail card

When applying the search algorithm for unused spaces to this e-mail card, a lot of unused spaces will be found in it. A part of these unused spaces is shown in figure (6).

```
64 25 C1 91 53 3A 05 68  15 FF F1 61 21 A0 A9 27  d%..S:.h...a!..'
FF F5 1A AD 25 50 0D 80  10 68 26 1B 09 30 84 8D  ....%P...h&..0..
39 0C 34 23 E1 11 0C 0C  22 34 22 68 41 26 8A CC  9.4#...."4"hA&..
98 4B 91 93 4C CB FF FA  11 9A 10 49 A1 1D 11 A6  .K..L......I....
7F AD CA 19 03 C3 FF FA  C5 4C 84 9B FA 00 A1 43  ¿........L.....C
41 52 23 12 2C 69 9D A0  C8 90 D6 B3 20 00 00 00  AR#.,i...... ...
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 FF F3 70 50 C4 08 C0  03 5A BB 04 00 01 12 59  .ÿ.pP....Z.....Y
B6 B5 EC 08 44 DC 00 00  00 00 00 00 00 00 00 00  ....D...........
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 20 00 20 00 20 00 20  ......... . . .
00 20 00 20 00 20 00 20  00 20 00 20 00 20 00 20  . . . . . . . .
```

Figure (6) Part of the unused spaces found in the e-mail card structure

After hiding the message "**Hide in SWF file**" directly in the above part of the unused spaces of the e-mail card structure, it will be shown in figure (7).

```
64 25 C1 91 53 3A 05 68  15 FF F1 61 21 A0 A9 27  d%..S:.h...a!..'
FF F5 1A AD 25 50 0D 80  10 68 26 1B 09 30 84 8D  ....%P...h&..0..
39 0C 34 23 E1 11 0C 0C  22 34 22 68 41 26 8A CC  9.4#...."4"hA&..
98 4B 91 93 4C CB FF FA  11 9A 10 49 A1 1D 11 A6  .K..L......I....
7F AD CA 19 03 C3 FF FA  C5 4C 84 9B FA 00 A1 43  ¿........L.....C
41 52 23 12 2C 69 9D A0  C8 90 D6 B3 20 48 69 64  AR#.,i...... Hid
65 20 69 6E 20 53 57 46  20 66 69 6C 65 00 00 00  e in SWF file...
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 FF F3 70 50 C4 08 C0  03 5A BB 04 00 01 12 59  .ÿ.pP....Z.....Y
B6 B5 EC 08 44 DC 00 00  00 00 00 00 00 00 00 00  ....D...........
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 20 00 20 00 20 00 20  ......... . . .
00 20 00 20 00 20 00 20  00 20 00 20 00 20 00 20  . . . . . . . .
```

Figure (7) Hiding the Message (plain Text) in e-mail card structure

If the attacker suspects about this e-mail card and tries to open its structure, the hidden message (plain text) will be exposed. Therefore the hidden message must be scrambled in order to confuse the attacker by using one of the encryption techniques.

In order to encrypt the message before hiding it, RSA public key encryption is used, its goal is to have a method for transmitting a secret code without having to worry about eavesdropping. This technique is done automatically in the proposed system when the user saves (hides) the message in the e-mail card.

If the message "**Hide in SWF file**" is encrypted by using the above method, no one will see the sending concealed data with the e-mail card, but if someone happens to stumble on it, at least it is encrypted, so it won't be easily cracked as in figure (8).

```
64 25 C1 91 53 3A 05 68  15 FF F1 61 21 A0 A9 27  d%..S:.h...a!..'
FF F5 1A AD 25 50 0D 80  10 68 26 1B 09 30 84 8D  ....%P...h&..0..
39 0C 34 23 E1 11 0C 0C  22 34 22 68 41 26 8A CC  9.4#...."4"hA&..
98 4B 91 93 4C CB FF FA  11 9A 10 49 A1 1D 11 A6  .K..L......I....
7F AD CA 19 03 C3 FF FA  C5 4C 84 9B FA 00 A1 43  ¿........L.....C
41 52 23 12 2C 69 9D A0  C8 90 D6 B3 20 53 47 6C  AR#.,i...... SGl
6B 5A 53 42 78 62 69 42  54 56 4F 59 67 5A 6D 6C  kZSBxbiBTVOYgZml
73 5A 51 00 00 00 00 00  00 00 00 00 00 00 00 00  sZQ.............
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 FF F3 70 50 C4 08 C0  03 5A BB 04 00 01 12 59  .ÿ.pP....Z.....Y
B6 B5 EC 08 44 DC 00 00  00 00 00 00 00 00 00 00  ....D...........
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00  00 20 00 20 00 20 00 20  ......... . . .
00 20 00 20 00 20 00 20  00 20 00 20 00 20 00 20  . . . . . . . .
```

Figure (8) Encrypting the Message using RSA encryption

In order to make the ciphered message more secure to attack, it will be covered by a password which is optional, when selecting the password the ciphered message will be encrypted once again by using XOR encryption with the password as a key and then the password and the resulted ciphered message will be XOR encrypted with the size of the selected e-mail card in order to confuse the attacker, the password will reside in the first free blocks after

the header. The reasons for using the size of the selected e-mail card as a key, is it is always different from one e-mail card to another.

When the XOR encryption is applied to the ciphered message (RSA encrypted) by using the password for example "flash card", the resulting ciphered message will be shown as in figure (9).

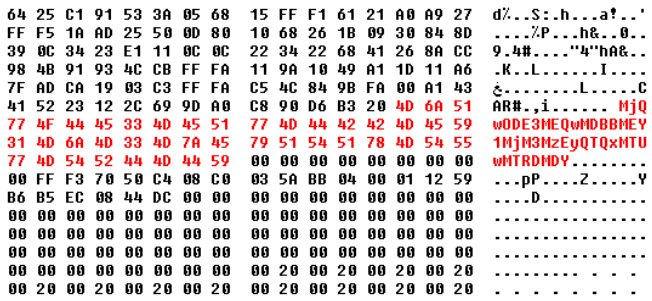

Figure (9) Encrypting the ciphered Message using XOR encryption

The Hiding algorithm is shown below:

Input: Message (Plain text), E-mail card (cover).

Output: Stego E-mail card.

Step 1: Open the e-mail card structure (SWF file) in binary mode.

Step 2: If there are no spaces found in e-mail card structure then choose another e-mail card and goto Step 1.

Step 3: Input the message

Step 4: Read the array which contains the indexes of the beginning and the ending of the blocks of spaces, also the number of spaces.

Step 5: If the entered message is not equal to or less than the available spaces for hiding then the input message should be edited to be equal to or less than the available spaces goto Step 3.

Step 6: Encrypt the message using RSA Encryption method.

Step 7: If there is no password then goto step 8. Else Apply XOR encryption to the ciphered message (RSA encrypted) with the password s a key and apply XOR encryption once again (to the resulted ciphered message and password) with the size of the E-mail card as a key.

Step 8: Partition the resulted encrypted message according to the locations of the blocks of Spaces in the e-mail card structure (SWF file).

Step 9: Delete all the spaces in the array.

Step 10: Hide (Save) the message in the e-mail card.

Step 11: Stop.

3.5. Extracting Process:

When the Stego-Object (e-mail card) transmitted to the recipient, who in his way wants to extract the hidden message from its structure, the e-mail card should be loaded in the proposed system in order to do this.

The proposed system will automatically looking for a hidden message in the e-mail card structure by reading its header and excludes it. Then the first block after the header will be checked for the password (which sign is "~💡") , if it is found that means there is a hidden

message covered by password (the starting sign of the password is "|°") otherwise (if the sign is "N0p455w" means no password found) the proposed system will look for the starting index of the hidden message, by taking one byte at a time if it is related to the lookup table it will be ignored else checking if it is a starting data index (which sign is "°|") to the hidden message that means there is a hidden message (RSA encrypted only), then read the byte or bytes after it, collect them into a block until reaching to the ending data index (which sign is "|]"), the searching will continue until reaching to the end of the e-mail card structure, else there isn't any hidden message.

After that the proposed system will start to extract the ciphered message from the e-mail card structure, if it is covered by password, XOR decryption will be applied to the SWF file by using the size of the e-mail card as a key to get the password. The password will be truncated from the SWF file, and XOR encryption will be applied to the SWF file using the size of the e-mail card as a key in order to return the hidden message back to its form. A check will be done for the correct password; if it is not correct then it must be entered once again. Now the password is used as a key and then it is XOR decrypted with the hidden message to get the ciphered message (RSA encrypted), finally RSA decryption will be applied to the ciphered message to gain the original message (plain text). In case there isn't password in the e-mail card structure, only RSA decryption will be applied to the ciphered message to gain the original message (plain text).

The extracting algorithm is shown below:

Input: Stego E-mail card

Output: Message (Plain Text)

Step 1: Open the e-mail card structure (SWF file) in binary mode and search.

Step 2: Check for password, If there isn't password then goto step 8.

Step 3: Get the Length of the e-mail card (SWF file).

Step 4: Apply XOR decryption to the SWF file using the length of the e-mail card (file size) as a key to get the password.

Step 5: Truncate the password from the SWF file.

Step 6: Apply XOR Encryption to the SWF file using the length of the e-mail card (file size) as a key.

Step 7: Check,

If the password correct then Apply XOR Decryption to the hidden message using the password as a key to get the RSA encrypted message, Goto to step 9.

Else

If the password isn't correct after three trials then goto step 11.

Step 8: Check for Indexes:

If there isn't Indexes then that mean there isn't any hidden message, select another e-mail card and goto step 1.

Step 9: Apply RSA Decryption to the encrypted message to get the original message (plain text).

Step 10: Display the message (plain text) in the writing box of the proposed system to be read.

Step 11: Stop.

6. Experimental Test and Results:

There are various forms of e-mail cards for greetings that designed from only text or may be with sound or picture or all of them and the size of the unused spaces available in these e-mail cards structures (carrier) for hiding depends on the media used in it, as shown in the e-mail cards in the below sections.

6.1. E-Mail Card (Animation, Text, Image (Still & Moving) & Song):

The whole size of this e-mail card is (447500) bytes and the size of the actual unused spaces is (11220) bytes but the number of the allowed spaces of characters (bytes) can be used for hiding is (448) character as a message, as shown in figure (10).

Figure (10) E-Mail Card (Animation, Text, Image (Still & Moving) & Song)

When the user writes the message in the writing box of the proposed system, whose length is 257 characters. The whole e-mail card size after the hiding process is (447500) bytes according to the hidden message.

Dear Sir:

The formula has been tested and proven successful: place contents into packaging, seal package, apply label with recipient information to the package face, and attach [1]completed shipping form.

Thank you as always for your cooperation.

Regards

6.2. E-Mail Card (Animation, Text, Still Image & Music):

The whole size of the e-mail card is (415089) bytes and the size of the actual unused spaces is (4462) bytes but the number of allowed spaces of characters (bytes) can be used for hiding is (557) character as a message, as in figure (11).

Figure (11) E-Mail Card (Animation, Text, Still Image & Music)

When the user writes the message in the writing box of the proposed system, whose length is 447 characters. The whole e-mail card

[1] ١

size after the hiding process is (415089) bytes according to the hidden message.

نص القانون بانه يجب حماية المعلومات ذات القيمة المالية من مخاطر الانماط الجرمية المستجدة التي تعتمد الكمبيوتر وسيلة للجريمة او هدفا او بيئة لها ، وهو ما عرف ايضا بجرائم الكمبيوتر Computer Crimes أو الجرائم المرتبطة بالكمبيوتر Computer-Related Crimes او جرائم الكمبيوتر ذات الطبيعة الاقتصادية Economic Computer Crimes , او غير ذلك من اصطلاحات دالة عليها، ويقع ضمن نطاق دراسات القانون الجنائي الموضوعي وهو ما عبر عنه بالعموم بوصفه الحق في المعلومات

6.3. E-Mail Card (Animated Text & Still Image):

The size of the e-mail card is (38660) bytes and the size of the actual unused spaces is (0) bytes and the number of allowed spaces of characters (bytes) can be used for hiding is (0) character, as shown in figure (12).

This is a special case which shows there are no spaces in this type of the e-mail card.

Figure (12) E-Mail Card (Animated Text & Still Image)

6.4. E-Mail Card (Animated Text, Still Image & Music):

The whole size of the e-mail card is (331664) bytes and the size of the actual unused spaces is (3442) bytes but the number of the allowed spaces of characters (bytes) which can be used for hiding is (430) character as a message, as shown in figure (13).

Figure (13) E-Mail Card (Animation, Text & Moving Image)

When the user writes the message in the writing box of the proposed system, whose length is 134 characters. The whole e-mail card size after the hiding process is (331664) bytes according to the hidden message.

There will be lots of attacks that cause all sorts of problems. But the “devastation” will be less than the government likes to paint.

6.5. E-Mail Card (Animation, Text & Music):

The whole size of the e-mail card is (68578) bytes and the size of the actual unused spaces is (1147) bytes but the number of the

allowed spaces of characters (bytes) which can be used for hiding is (143) characters, as shown in figure (14).

Figure (14) E-Mail Card (Animation, Text & Music)

When the user writes the message in the writing box of the proposed system, whose length is 134 characters. The whole e-mail card size after the hiding process is (68578) bytes according to the hidden message.

انصحك بعدم فتح الملفات التي تنتهي بأحد هذه الاختصارات
وخاصة إذا لم تكن من شخص معروف
COM= Command Files.
APP= Application.
BAT= Batch Files.

6.6. E-Mail Card (Animation, Text & Moving Image):

The whole size of the e-mail card is (28567) bytes and the size of the actual unused spaces is (255) bytes but the number of the allowed spaces of characters (bytes) which can be used for hiding is (31) character as a message, as shown in figure (15).

Figure (15) E-Mail Card (Animation, Text & Music)

When the user writes the message in the writing box of the proposed system, whose length is 30 characters.

Send money as soon as possible

The whole e-mail card size after the hiding process is (28567) bytes according to the hidden message.

7. E-mail Cards Comparative Study:

From the previous different practical examples there are many results and remarks can be obtained. Table (2) contains the sizes of cover file (the e-mail card), the size of the hidden message and the size of stego file.

Table (2): Comparison between the results

Index	Section	Size of Cover (E-card) Before Hiding Process	Size of the spaces available in E- card	No. of character possible used	Size of the Hidden Message	Size of Stego (E-card) After Hiding Process
1	4.2.	447500 B	11220 B	448 B	257 B	447500 B
2	4.3.	415089 B	4462 B	557 B	447 B	415089 B
3	4.4.	38660 B	0 B	0 B	---------	----------
4	4.5.	331664 B	3442 B	430 B	134 B	331664 B
5	4.6.	68578 B	1147 B	143 B	143 B	68578 B
6	4.7.	28567B	255 B	31 B	30 B	28567B

From table (2) there are many remarks can be obtained:

1. The size of the unused spaces in the e-mail card to use in hiding depends on the media used to design the e-mail card such as (sound, moving image and animation) as in sections 6.1, 6.2, 6.4.
2. If the size of the hidden message is larger than spaces available, it is not acceptable process.
3. In all examples above, the hiding process does not effect the e-mail cards presentation, which means the message (hidden in the SWF file) will be perceived to be as close as possible to the original carrier by the human senses, the size of the SWF file after the hiding process as shown in column (7) remain the same as the size of the SWF file before the hiding process which will not draw any suspicion.
4. If the E-mail card is designed by using just text (animated or not) or still image or both, the final E-mail card will be without spaces as in section 6.3 or may be possible with little spaces.

8. Conclusions:

The increased usage of E-mail, the augmentation of using the e-mail cards for greetings and advertisings nowadays, and the privacy of widely used Macromedia Flash (SWF file) in Internet, have caused need for a system which employs the above factors in hiding.

1. Different types of e-mail cards have been studied for the possibility of using them in hiding and it is found that the e-mail card which consists of sound, animation and moving image is good for hiding (because it contains many spaces available for hiding).

2. Since Macromedia Flash (SWF) is used in designing the e-mail cards, the size of these e-mail cards is different depending on the media used, in the case of the e-mail card which is in a large size, there is a simple delay in time when loading it from directory, because the program will automatically look for suitable places (unused spaces) for hiding the message in it. At the same time, at most the large size of the e-mail card is good for giving us suitable places enough to hide a regular message.

3. It has been found that the hidden message will be perceived to be as close as possible to the original carrier (e-mail card) by the human senses without drawing any suspicion.

4. Using cryptography supports the security immunity of the proposed hiding system without causing any additional distortion.

5. For more security the e-mail card is used only once for hiding a message in it, therefore

usually there is a directory which contains different unused e-mail cards to select.

6. The proposed system is successfully tested between two sites by attaching the e-mail card which contains a hidden message via e-mail services through the internet.

7. The achieved time to encrypt the message "Hide in SWF file" has been calculated outside the program, it takes 6 seconds to encrypt the message by using RSA encryption method only and it takes 34 seconds to encrypt the message by using both RSA encryption method and XOR encryption method (password is "flash card") respectively, therefore only a very small amount of data expansion is involved when using RSA encryption.

9. References:

[1] Fabien A. P. Petitcolas, Ross J. Anderson and Marku G. Kuhn, **"Information Hiding-A Survey"**, Proceedings of the IEEE, Special Issue on Protection of Multimedia Content, (7):1062{1078, 1999.

[2] **"WEPIN Store, Steganography (HiddenWriting)"**, Copyright at Common Law, West El Paso Information Network, 1995. *http://www.wepin.com/pgp/stego.html*

[3] Vidas A., "**Data Hiding: A Policy and Futures Overview of Digital Watermarks and Steganography**", 2002. *http://www.unc.edu/~vidaa/inls281/281howwork.html*

[4] "**Steganography**", A Word Definition From the Webopedia Computer Dictionary, 2004. *http://www.webopedia.com/TERM/S/steganography.html*

[5] Hosmer C. and Hyde C., **"Discovering Covert Digital Evidence",** WetStone Technologies, Inc., DFRWS, 2003.

[6] **"eCards"**, E-Marketing Associates, 2004. *http://www.e- marketingassociates.com/ecards/ecard-main.asp*

[7] **"Market your products/services with ecards"**, Hosted by FullServeHost.com -- professional web hosting, Powered by vCard Lite 3.0.5, 2003. *http://www.humordrive.com/ecards/*

[8] **"Macromedia Flash on the Internet"**, 2003. *http://www.flash.htm*

[9] BEng III Simon Wistow, **"Deconstructing Flash/Investigations in to the SWF file format"**, Simon Wistow BEng III <smw3@doc.ic.ac.uk>, 2000.

[10] **"Macromedia Flash File Format (SWF)"**, 2003. *http://www.half-serious.com/swf/format/*