ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Digital Steganography through Enhanced Multi-Party Covert Communication

Jithesh K[1],* S.B Kishor[2], Pradeep K Butey[3]
[1]Department of Electronic & Computer Science, R.T.M. Nagpur University, Nagpur.
[2]Department of Computer Science, Sardar Patel Mahavidyalaya, Chandrapur, India.
[3]Department of Computer Science, Kamala Nehru College, Nagpur, India.
***Corresponding author: E-Mail: jithukotheri@gmail.com**

In this paper, we try to enhance and fault proof the "multi-party covert communication with steganography and quantum secret sharing", proposed by Liao by gracefully importing certain missing conditions. It is a stronger notion of security than standard secure multi-party communication. Multi-party covert communication guarantees that the process of it cannot be observed. As of now this scheme has little detection risk. But the missing things may lead to the failure of the communication or it may lead to an incorrect communication. Hence, we propose an enhanced version of the Liao's scheme that guarantees a complete communication without error or failure. This scheme proposes a steganographic communication based on a channel hidden within quantum secret sharing (QSS). To an outside observer, participants will engage in a typical instance of QSS, just like the others. But when the session is over, covert multi-party communication has already been done.

KEY WORDS: Multi-party covert communication, Steganography, Payload, Quantum secret sharing, steganalysis.

1. INTRODUCTION

In computer security, a covert channel is a type of computer security attack that creates a capability to transfer information objects between processes that are not supposed to be allowed to communicate by the computer security policy. The term, proposed in 1973 by Lampson. Steganography has become more noteworthy as more and more people join the cyberspace revolution (Hillery, 1999). Steganography is an information hiding technique whereby the information is masked inconspicuously inside a host data set in such a way that its presence is barely visible (Gottesman, 2000). Digital audio, video, and images are commonly used carriers for furnishing the information. Scientifically steganographic embedding can be modeled as

$$f(C, X, K) = Z \quad (1)$$

The function f represents the steganographic function that decides how the secret message X will be embedded into cover-object C. Key K is to ensure that the recipient who knows the corresponding decoding key will be able to extract X from stego object Z. Similarly decoding will be

$$f'(Z, K) = X \quad (2)$$

f 'characterizes the decoding function corresponding to f. Additionally the function f should generally possess three important characteristics to facilitate a reliable covert channel including high payload capacity for transferring large quantity of secret data, good perceptual quality to ensure security against visual attacks and resistance to steganalysis strategies to ensure security against statistical attacks.

Preliminaries: A quantum version of steganography is a method based on quantum physics. Quantum steganography can be separated into two types. One is called Quantum Multi secret Sharing (QMS) (Hillery, 1999; Gottesman, 2000; Eggeling, 2002; Terhal, 2001) which can be generalized to hide the bits in multipartite quantum states for exchanging secret messages. In this type of quantum steganography the bits are superimposed in the way that the other end can recover the bit by means of local operations and conventional communications. The other one is called Quantum Data Hiding (QDH) (Banacloche, 2004; Worley, 2004; Matin, 2007; Mogos, 2008, 2009) which builds up logical channel within normal quantum channel to transmit secret. It is easy to see that QDH is more closely associated with traditional steganography than QMS and can more successfully communicate secret messages. In their study Liao et al clearly mentioned the transition of secret conveyance from conventional steganography to quantum steganography with the following case in points. In 2002, Banacloche (2004) adopted QECC (Quantum Error- Correcting Code) to hide secret messages as errors in arbitrary quantum data files. In this protocol, secret messages could also act as watermarks to secure authenticity or integrity of the data. In 2004, G. G. Worley III (2004) proposed a new quantum watermarking, which embedded digital watermark by introducing errors in measurement results based on QKD (Quantum Key Distribution), BB84 protocol (Bennett, 1984). In 2007, Matin(2007) presented a novel quantum steganographic communication protocol. It analyzed imperceptibility and security in detail, and accurately calculated capacity of this type of hidden channel. In 2008 Mogos (2008) proposed another new quantum steganography based on quantum teleportation. It used three-dimensional qubits to represent RGB (Red, Green and Blue) pixels for transmitting the quantum secret messages in digital color images. As a result, it successfully extended steganography from classical channel to quantum channel. After that, Mogos (2009) made further improvements on this algorithm in 2009.

A bit is the basic unit of information in computing and digital communications. A bit can have only one of two values, and may therefore be physically implemented with a two-state device. These values are most commonly

represented as either a 0 or 1. The term bit is a portmanteau of binary digit. Quantum computation and quantum information are built upon an analogous concept: the quantum bit (qubit or qbit for short). The concept of the qubit was unknowingly introduced by Stephen Wiesner in 1983. But the name quibit was attributed to Benjamin Schumacher. Identical to a classical bit, a qubit also has a state. In a classical system, a bit would have to be in one state or the other. A pure qubit state is a linear superposition of the basis states. This means that the qubit can be represented as a linear combination of $|0\rangle$ and $|1\rangle$:

$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$

where α and β are probability amplitudes and can in general both be complex numbers satisfying

$|\alpha|2 + |\beta|2 = 1$,

which correspond to the states 0 and 1 for a conventional bit. . However quantum mechanics allows the qubit to be in a superposition of both states at the same time, a property which is fundamental to quantum computing. When a qubit is measured with an orthogonal basis, it only gives "0" or "1" as the measurement result. An observer can specify what they want to measure by specifying a basis. Two examples of basis are: standard or the computation basis Z = {$|0\rangle$, $|1\rangle$} and the Hadamard rotated basis X = {$|+\rangle$, $|-\rangle$}. $|+\rangle = (1/\sqrt{2})(|0\rangle + |1\rangle)$ and $|-\rangle = (1/\sqrt{2})(|0\rangle - |1\rangle)$ correspond to the states 0 and 1 for a classical bit. When we measure a state described by the qubit $|\psi\rangle = \alpha|0\rangle + \beta|1\rangle$ in the Z basis, we get either the result $|0\rangle$, with probability $|\alpha|2$, or the result $|1\rangle$, with probability $|\beta|2$. Table 1 summarizes the measurement results of the states $|0\rangle$, $|1\rangle$, $|+\rangle$and $|-\rangle$ in the Z basis and X basis, respectively.

Table.1.The measurement results of the states in the different basis

States	Z Basis	X Basis
$\|0\rangle$	0	0 with probability 1/2,
$\|1\rangle$	1	1 with probability 1/2
$\|+\rangle$ 0 with probability 1/2, 1 with probability 1/2		0 with probability 1/2, 1 with probability 1/2
$\|-\rangle$ 0 with probability 1/2,		0
1 with probability 1/2		1

Literature Review: Our main intention is to include a few conditions that were missed in the study of Liao et al's Multli-party covert communication (Liao, 2010). In this subsection, we briefly describe Liao's scheme (Liao, 2010), which is an extended version of Guo's QSS scheme (Guo, 2003). Here Liao present a novel multi-party covert communication scheme by gracefully integrating steganography into Guo's QSS. In their method every run except the first could covertly multiparty communicate 1-bit secret. Before the covert communication takes place, they agree up on two integer's d ($1 \le d \le n$) and $r \in \{0, 1\}$ in advance. They don't covertly communicate secret bits in the first run. In the j-th ($j \ge 2$) run, Alice uses m-bit key ka = (k0, k1, · · ·, km-1) ($ki \in \{0,1\}$) generated in the previous run to update d and r:

r = km-1 (2)

$$d = \left(\sum_{i=0}^{m-2} k_i \, X \, 2^i \ mod \ n\right) + \ 1 \quad (3)$$

We make a few modifications to Liao et al.'s scheme. They missed few situations that are to be noticed before committing a transaction. So that an outside observer can be oblivion of covert communication as well as the communicating entity can assure the correctness of the information. The coding qubits in the corresponding basis of by Liao et al.'s scheme is shown in table 2.

Table.2.The coding quibits in the corresponding basis

l	0		1	
a	0	1	0	1
bc	00	01	00	10
	11	10	11	01
BC	$\|0\rangle\|0\rangle$	$\|0\rangle\|1\rangle$	$\|+\rangle\|+\rangle$	$\|-\rangle\|+\rangle$
	$\|1\rangle\|1\rangle$	$\|1\rangle\|0\rangle$	$\|-\rangle\|-\rangle$	$\|+\rangle\|-\rangle$

The following section briefly describe Liao et al.'s scheme that was derived from Guo's QSS scheme:

Alice generates two random 2n-bit strings l = (l1, l2, · · ·, l2n) and a = (a1, a2, · · ·, a2n). She randomly selects a "steganographic bit" aq ($1 \le q \le 2n$) whose value equals to the XOR result of Alice's secret bit s and r.

$aq = s \oplus r$ (4)

For each bit of l and a, she creates qubits Bi and Ci in the Z basis (if li =0) or X basis (if li = 1), where $bi \oplus ci = ai$. Table 2 summarizes the coding qubits in the corresponding basis. For example, if li = 1 and ai = 0, Alice prepares either Bi = Ci = $|+\rangle$ (bi = ci =0) or Bi = Ci = $|-\rangle$ (bi = ci = 1) each with probability 1/2. But she knows exactly which pair of qubits she prepares. She sends 2n-qubit strings B = (B1, B2, · · ·, B2n) and C = (C1, C2, · · ·, C2n) to Bob and Charlie, respectively.

When both Bob and Charlie announce that they have received their strings, Alice announces l. Bob and Charlie measure each qubit in the Z basis or X basis according to the corresponding bit value of l.
In this step, Alice will select n check bits in a. The first n−1 check bits from the 2n−1 bits (aq is excluded from the original 2n bits) are randomly selected, while the last one is chosen intentionally.
Suppose the remaining n + 1 bits are v = (v0, v1, v2, · · ·, vn) and the "steganographic bit" is vt (i.e. aq in a). The last check bit vx is chosen such that

$$x = (t - d) \bmod (n + 1) \quad (5)$$

Bob and Charlie are required to announce the measurement results of their corresponding check qubits in B and C.
If Alice finds the number of agreed values is unacceptably few, she aborts this run and restarts from step 1. Otherwise, she continues to the next step.
They perform information reconciliation and privacy amplification to generate three m-bit keys ka, kb and kc from the remaining n bits. Alice, Bob and Charlie can obtain ka, kb and kc separately, where ka = kb ⊕ kc . Alice's secret bit s can be obtained by Bob and Charlie cooperatively. They first reconstruct ka by their separated keys kb and kc, then obtain r and d by Eqs. (2) and (3). The correct location of the
"Steganographic bit" vt can be derived by

$$t = (x + d) \bmod (n + 1) \quad (6)$$

Where, x is announced in step 3. They implement the operation cooperatively.

$$s = bq \oplus cq \oplus r \quad (7)$$

Proposed Enhanced Steganography through Multi Party Covert Communication: In this subsection, we enhanced the multiparty covert communication scheme proposed by Liao et al.'s scheme adding missing conditions that otherwise compromise the security of the communication system. We added the following constraints so as to ensure and improve the accuracy of the secret to be received. Also it can minimize the number of aborting run due to unacceptable values.

$$x = |t - d| \pmod 7. \quad (8)$$

The check bits may not be consecutive.
q can be zero. It is mentioned in the step (1) of Liao's scheme that ($1 \leq q \leq 2n$).
But example 2 shows q can be 0.
From the experiment we observed that d can be greater than n. If the value of the d is greater than n then

$$d = d \bmod 6 \quad (9)$$

In the equation (7) it is mentioned that the secret bit s= bq ⊕ cq ⊕ r. The equation (10) is also found to be true. That is in the following illustration s=0, bq=0 and cq=0. Assigning these values to the equation (7) then s will be 0. Hence the equation can be written as

$$S = bq \oplus cq \quad (10)$$

Where, "⌐" represents the last quibits.
The same example illustrated in their study by Liao et al was used here for validating the modified algorithm as well as better comparison. The twelve-bit strings l and a (n=6) are supposed to be 011010010001 and 010011101101, and Alice's secret bit s = 0. Suppose five-bit key ka (m= 5) generated in the previous execution is 01111, then r = 1 and d = 3. Alice randomly selects the "steganographic bit": 010011101101, where the bit marked in bold face denotes the "steganographic bit". She creates the strings:
B = |1⟩ |−⟩ |−⟩ |0⟩ |+⟩ |1⟩ |1⟩ |−⟩ |0⟩ |0⟩ |0⟩ |+⟩
C = |1⟩ |+⟩ |−⟩ |0⟩ |−⟩ |0⟩ |0⟩ |−⟩ |1⟩ |1⟩ |0⟩ |−⟩
During validation steps, Alice arbitrarily selects five check bits at first: 0 1 * 0 1 * 1* * 1 0 *, corresponding to
B = |1⟩ |−⟩ * |0⟩ |+⟩ * |1⟩ * *|0⟩ |0⟩ *
C = |1⟩ |+⟩ * |0⟩ |−⟩ * |0⟩ * *|1⟩ |0⟩ *
Where, five check quantum bits are denoted by "*". As per the case in point the remaining seven bits are v0v1v2v3v4v5v6 = 0101110. Alice selects the last check bit using the first proposed condition that is equation (8).
$x = |t - d| = 5 - 3 = 2 \pmod 7$. The last check bit is v2, corresponding to
B = |1⟩|−⟩ *|0⟩|+⟩ * |1⟩ * *|0⟩|0⟩*
C = |1⟩|+⟩ *|0⟩|−⟩ * |0⟩ * *|1⟩|0⟩*
Where, the last check qubits are marked by "⌐".
Example: The same example of Liao et al is used for illustrating the condition c and the equation (10) of the proposed scheme of improved multiparty communication. The twelve-bit strings l and a (n=6) are supposed to be the previous one, that is 011010010001 and 010011101101, and Alice's secret bit s = 1. Suppose five-bit key ka (m= 5) generated

in the previous execution is 01011, then r = 1 and d = 5. Alice randomly selects the "steganographic bit": 010011101101, where the bit marked in bold face denotes the "steganographic bit", aq. She creates following strings:
B = |1⟩ |−⟩ |−⟩ |0⟩ |+⟩ |1⟩ |1⟩ |−⟩ |0⟩ |0⟩ |0⟩ |+⟩
C = |1⟩ |+⟩ |−⟩ |0⟩ |−⟩ |0⟩ |0⟩ |−⟩ |1⟩ |1⟩ |0⟩ |−⟩
During the checking procedure, Alice randomly selects five check bits at first: 0 1 * 0 * 1* 0 * * 0 1, corresponding to
B = |1⟩|−⟩ * |0⟩ * |1⟩ * |–⟩ * * |0⟩|+⟩
C = |1⟩|+⟩ * |0⟩ * |0⟩ * |–⟩ * * |0⟩|–⟩
Where, five check (qu) bits are denoted by "*". The remaining seven bits are v0v1v2v3v4v5v6 = 0101001. Alice selects the last check bit by the method mentioned earlier. $x = |t - d| = |0 - 3| = 3(\text{mod}7)$. The last check bit is v3, corresponding to
B = |1⟩|−⟩ * |0⟩ * |1⟩ * |–⟩ * * |0⟩|+⟩
C = |1⟩|+⟩ * |0⟩ * |0⟩ * |–⟩ * * |0⟩|–⟩
Where, the last check qubits are marked by "⌐".
From this illustration it is clear that aq can be zero. Hence the condition (c) in the improved version is verified. The equation (10) is also verified in this case in point. That is here s=1, Bq=1 and Cq=0.
Security analysis: There are two different kinds of attacks: an outside observer who wants to eavesdrop on Alice's secret without being detected, and a dishonest member of Bob–Charlie pair, who tries to extract sender's secret without collaborating with the other one. Without loss of generality, suppose the dishonest member is Bob. Neither of them is able to acquire sender's secret, even if either Eve guesses the covert communication is underway or Bob eavesdrops. There is only one possibility of a successful attack and it happens when the Bob-Charlie pair together becomes dishonest. The security of Liao et al.'s scheme becomes complete only with the proposed improvements. Otherwise the main objective of the secret communication is compromised. The scheme proposed by Liao et al. also satisfies the other three requirements: cooperatively, covertness, and scalability. But it lacks robustness. The improved version ensures this and also provides high reliability.

2. CONCLUSION

In this paper we propose an improved version of multi-party covert communication scheme proposed by Liao's, based on a steganographic channel hidden within a conventional QSS scheme. Though they are few the modifications made are very important as far as a covert communication is taking place. The main triple pillars of a secret communication are confidentiality, integrity and proper availability. Before the enhancement the availability of the secret was not guaranteed. It also assures robustness and reliability to the previous work. Even if either an outside observer guesses the covert communication is carrying on or a dishonest member of participants is eavesdropping, it is proved that he gains nothing about hidden information. Furthermore, it is secure against current steganalysis techniques. Often intruders are anticipating a cover medium when steganography takes place. Here, in view of the fact that no physical medium is required the usual steganalysis are worthless. However, this scheme is not suitable for large payload communication. Here in each transaction only a single bit is communicated. So our future work will concentrate to improve the capacity of each transmission.

REFERENCES

Banacloche JG, Math J, Quantum Error correcting Code, Physical review letters, 291, 2009, 813.

Eggeling T, Werner RF, Physical Review Letters, 89, 2002, 097905.

Gottesman D, Physical Review Letters, 61, 2000, 042311.

Hillery H, V. Buzek A, Berthiaume, Physical Review A, 59, 1999, 1829.

Matin K, Proc. of 9th Information Hiding workshop, 2007, LNCS 4567, 32

Mogos G, Int. J. Multimedia Ubiquitous Eng, 4, 2009, 13.

Terhal B.M, Vincenzo D, Leung D.W, Physical Review. Letters, 86, 2001, 5807

Worley III GG, Quantum watermarking by frequency of error when observing qubits in dissimilar bases, arXiv, 2004, 040104

Xin Liao, Qiao-yan Wena, Ying Suna, Jie Zhangb, Multi-party covert communication with steganography and quantum secret Sharing, The Journal of Systems and Software, 83, 2010, 1801–1804

Zhi-Guo, Novel quantum steganography with large payload, Optics Communications, 283, 2010, 4782–4786.