DOI 10.15276/imms.v13.no1-2.56
УДК 004.056.5

Informatics and Mathematical Methods in Simulation
Vol.13 (2023), No. 1-2, pp.56-62

ПІДВИЩЕННЯ СТІЙКОСТІ СТЕГАНОГРАФІЧНОГО МЕТОДУ З КОДОВИМ УПРАВЛІННЯМ ВБУДОВУВАННЯМ ДОДАТКОВОЇ ІНФОРМАЦІЇ ДО АТАК ЗАШУМЛЕННЯМ

Д.О. Гулід, А.В. Соколов

Національний університет «Одеська політехніка»
Україна, Одеса, 65044, пр-т Шевченка, 1, radiosquid@gmail.com

Зростання обсягів мультимедійного контенту, що генерується, зберігається та передається сучасними інформаційними системами, призводить до збільшення ролі стеганографічної компоненти в системах захисту інформації. При цьому, до застосовуваних стеганографічних методів висуваються значні вимоги щодо їх ефективності, які включають достатню пропускну спроможність, забезпечення надійності сприйняття, стійкості до атак проти вбудованого повідомлення. Велике значення має швидкодія стеганографічного методу, особливо, якщо передбачається його застосування у режимі реального часу на ресурсообмежених платформах. Одним із сучасних стеганографічних методів, що характеризується забезпеченням основних показників ефективності при незначній обчислювальній складності через виконання стеганоперетворення у просторовій області контейнера, є стеганографічний метод з кодовим управлінням вбудовуванням додаткової інформації. Однак, незважаючи на досить високі показники стійкості до атаки зашумленням, яка може мати місце в багатьох практичних застосуваннях, актуальним лишається питання підвищення стійкості стеганоперетворення до даного типу атак. Метою роботи є підвищення стійкості до атак зашумленням стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації. У роботі розглянуто атаки проти вбудованого повідомлення зашумленням двома видами шумів: адитивним білим гаусовим шумом та шумом типу «Salt and Pepper». У роботі проведено експериментальне дослідження впливу структури застосовуваного кодового слова на стійкість стеганографічного методу з кодовим управлінням до атаки зашумленням адитивним білим гаусовим шумом, яке дозволило виробити практичні рекомендації щодо параметрів стеганографічного методу з кодовим управлінням в умовах даного типу атаки. Запропоновано застосування методу ШОВ (широкосмуговий сигнал, обмежувач, вузькосмуговий сигнал) для підвищення стійкості стеганографічного методу з кодовим управлінням до атак зашумленням шумом «Salt and Pepper», що дозволило знизити кількість помилок при вилученні додаткової інформації в умовах зашумлення даним шумом на 48%. Отримані у даній статті результати можуть бути корисними для застосування стеганографічного методу з кодовим управлінням на практиці в умовах передавання стеганоповідомлення по каналам, що характеризуються наявністю атак зашумленням проти вбудованого повідомлення.

Ключові слова: стеганографія, кодове управління вбудовуванням інформації, атака зашумленням, адитивний білий гаусів шум, шум «Salt and Pepper».

Вступ і постановка задачі. Важливим компонентом сучасних систем захисту інформації є стеганографічні методи, що забезпечують приховування самого факту наявності інформації, що захищається. На сьогодні, до застосовуваних стеганографічних методів висуваються суворі вимоги ефективності, що включають високу пропускну спроможність, забезпечення надійності сприйняття, стійкості до атак проти вбудованого повідомлення, а також низьку обчислювальну складність стеганоперетворення.

При цьому, вимога забезпечення стійкості стеганографічного методу до атак проти вбудованого повідомлення стає у протиріччя з вимогою забезпечення

низької обчислювальної складності через необхідність застосування просторів перетворень, перехід до яких потребує значних обчислювальних витрат (перш за все, сингулярного розкладання матриць блоків контейнера [1…5]), тоді як у більшості випадків методи, що застосовують для стеганоперетворення просторові області контейнера [6…8], є нестійкими до атак проти вбудованого повідомлення.

Вирішенням даного протиріччя стала розробка стеганографічного методу з кодовим управлінням вбудовуванням додаткової інформації (ДІ) [9], що працює у просторовій області контейнера та при цьому є здатним забезпечити відповідність зазначеним критеріям ефективності навіть у більшій мірі, порівняно з відомими методами, що передбачають застосування областей перетворення. На сьогоднішній день відомо чимало атак проти вбудованого повідомлення, найбільш розповсюдженими серед яких є атаки стисненням, тим не менш, доволі часто на практиці зустрічаються атаки зашумленням різними видами шумів, що робить актуальною задачу підвищення стійкості стеганографічних методів до даного виду атак. Як показують проведені дослідження, стійкість стеганографічного методу з кодовим управлінням вбудовуванням ДІ до атак зашумленням окремими видами шумів може бути суттєво підвищена.

Метою роботи є підвищення стійкості до атак зашумленням стеганографічного методу з кодовим управлінням вбудовуванням ДІ.

Стійкість стеганографічного методу з кодовим управлінням вбудовуванням ДІ до атак зашумленням адитивним білим гаусовим шумом. З метою порівняння стійкості стеганографічного методу з кодовим управлінням вбудовуванням ДІ до атаки зашумленням адитивним білим гаусовим шумом (АБГШ) при застосуванні різних кодових слів був проведений наступний експеримент. У вибірку з 500 кольорових зображень з бази NRCS [10] виконувалося вбудовування ДІ із застосуванням кодових слів, що впливають на обрану трансформанту перетворення Уолша-Адамара, після чого отримане стеганоповідомлення піддавалося зашумленню АБГШ із різними рівнями дисперсії D і математичним очікуванням $M = 0$. Після атаки зашумленням здійснювалося вилучення ДІ і вимірювання кількості помилок, що сталися. Результати дослідження представлені у табл. 1, де інтенсивність зашумлення представлено у вигляді PSNR [11]. У табл. 1 для стислості показані лише декілька кодових слів кожного розміру, що вибірково впливають на задану трансформанту перетворення Уолша-Адамара.

Аналіз даних, що представлені у табл. 1 показує, що стійкість методу до атак зашумленням АБГШ не залежить від обраного кодового слова. Оскільки шум АБГШ має рівномірну спектральну щільність, це призводить до того, що вибір конкретного кодового слова не має значного впливу на стійкість методу.

Розкид значень відсотку помилок при атаці проти вбудованого повідомлення зашумленням АБГШ з різними значеннями дисперсії для різних кодових слів порядку μ з елементарною структурою $\{\mu(1), 0(\mu-1)\}$ становить: до 0.2% помилок для кодових слів розміру $\mu = 4$, до 0.1% помилок для кодових слів розміру $\mu = 8$ та до 0.3% помилок для кодових слів розміру $\mu = 16$.

При застосуванні кодового слова, яке впливає на постійну складову, відсоток помилок при декодуванні в умовах атаки зашумленням в середньому більший на 0.7% для кодових слів розміру $\mu = 4$, на 0.9% для розміру $\mu = 8$ і на 1.9% для розміру $\mu = 16$.

Таблиця 1

Залежність кількості помилок при вилученні ДІ від PSNR

Кодове слово / PSNR	6.9499	23.2094	30.0960	33.0817	35.2827	40.0017	42.9501	49.5088	61.1746
$N=4$									
$T_{4,(1,1)}$	49.7347	41.9107	32.1191	25.5330	19.8208	7.4452	2.5829	0.7541	0.6206
$T_{4,(1,2)}$	49.5007	41.6275	31.7966	25.1617	19.4106	6.9208	1.9746	0.0327	0
$T_{4,(1,3)}$	49.5107	41.6357	31.7908	25.1949	19.4223	6.9358	1.9887	0.0342	0
…									
$T_{4,(4,4)}$	49.5010	41.6453	31.7912	25.1672	19.4139	6.9157	1.9818	0.0324	0
$N=8$									
$T_{8,(1,1)}$	49.7010	34.1495	17.5188	9.4970	4.8697	1.0886	0.8595	0.6934	0.5338
$T_{8,(1,2)}$	48.9184	33.2513	16.6291	8.5859	3.9630	0.2255	0.0365	0	0
$T_{8,(1,3)}$	48.9328	33.2808	16.6394	8.5975	3.9916	0.2304	0.0380	0	0
…									
$T_{8,(8,8)}$	48.9279	33.2686	16.6103	8.5822	3.9681	0.2224	0.0353	0	0
$N=16$									
$T_{16,(1,1)}$	49.6422	21.6210	4.4085	1.7983	1.2713	0.9367	0.8081	0.6399	0.4615
$T_{16,(1,2)}$	47.7919	19.2586	2.6979	0.4183	0.0871	0.0035	0	0	0
$T_{16,(1,3)}$	47.8877	19.2815	2.7092	0.4186	0.0913	0.0035	0	0	0
…									
$T_{16,(16,16)}$	47.8049	19.2161	2.6898	0.4125	0.0898	0.0030	0	0	0

Зростання стійкості стеганографічного методу з кодовим управлінням вбудовуванням ДІ можливе лише за рахунок збільшення енергії кодового слова, тобто із застосуванням багаторівневих кодових слів [12].

На підставі результатів проведеного експерименту можна сформулювати наступні рекомендації щодо застосування стеганографічного методу з кодовим управлінням вбудовуванням ДІ в умовах атак зашумленням АБГШ:

1. Застосування багаторівневих кодових слів — за аналогією із вибором сигнальних конструкцій для роботи у каналах зв'язку, що зашумлені АБГШ, більша стійкість стеганографічного методу до атак зашумленням проти вбудованого повідомлення може бути забезпечена через збільшення енергії кодового слова шляхом застосування багаторівневих кодових слів.

2. Забезпечення впливу на високочастотні складові — задля забезпечення найбільшої надійності сприйняття стеганоповідомлення, зважаючи на рівний степінь стійкості кодових слів до атак зашумленням АБГШ, може бути рекомендоване застосування кодових слів, що впливають на найбільш високочастотні складові, наприклад, на трансформанту Уолша-Адамара (2,2). У разі застосування багаторівневих кодових слів, вибір даної трансформанти, для вбудовування ДІ також нівелює проблему знаходження максимальних за амплітудою елементів по краям кодового слова, що дозволить уникнути виникнення проблеми найбільшого перепаду яскравості на границях блоків та підвищити надійність сприйняття стеганоповідомлення.

Зазначені модифікації дозволяють адаптувати стеганографічний метод з кодовим управлінням вбудовування ДІ до роботи в умовах атак зашумлення АБГШ.

Стійкість стеганографічного методу з кодовим управлінням вбудовуванням ДІ до атак зашумленням шумом «Salt and Pepper». Для застосування стеганографічного методу з кодовим управлінням вбудовуванням ДІ в каналах з шумом типу «Salt and Pepper» можна рекомендувати додавання операції обмежування амплітуди матриць різниці Δ блоків стеганоповідомлення та оригінального контейнеру при вилученні ДІ. Це дозволить підвищити рівень стійкості стеганоповідомлення до таких атак.

Обмежування амплітуди матриць різниці полягає у встановленні її максимального значення, що відповідає максимальній амплітуді застосовуваного кодового слова. В разі використання бінарних кодових слів, максимальна амплітуда становить $\{\pm 1\}$. Цей підхід аналогічний відомому методу ШОВ, який ефективний для боротьби з імпульсними завадами.

Метод ШОВ (BAN, широка полоса — обмежувач — вузька полоса) є одним із підходів до фільтрації сигналів, зокрема використовується для боротьби з імпульсними завадами. Його назва вказує на його основні складові: широкосмуговий сигнал (Broadband), атенюатор (Attenuator) та вузькосмуговий сигнал (Narrowband) (рис. 1).

Рис. 1. Структурна схема ШОВ

Загальний принцип методу ШОВ може бути адаптований відповідно до специфічних вимог та властивостей шуму та сигналу у конкретній задачі, і, як показали проведені дослідження, може бути застосований для протидії шуму «Salt and Pepper» при застосуванні стеганографічного методу з кодовим управлінням вбудовуванням ДІ.

Так, відповідно до [9], при вилученні ДІ з стеганоповідомлення черговий блок Δ, у загальному випадку, може містити комбінацію з багатьох частот, що відповідає широкій смузі у методі ШОВ. Після цього здійснюється обмеження блоку за амплітудою значеннями $\{\pm 1\}$, і вже після цього — виділення конкретної частотної складової, що відповідає вузькій смузі у методі ШОВ.

Розглянемо конкретний приклад. Нехай блок спотвореного шумом типу «Salt and Pepper» з дисперсією $D = 0.1$ стеганоповідомлення S, а також відповідний йому блок оригінального повідомлення X, мають вигляд

$$X = \begin{bmatrix} 157 & 150 & 151 & 149 & 146 & 142 & 141 & 139 \\ 153 & 144 & 152 & 144 & 140 & 143 & 141 & 142 \\ 149 & 141 & 148 & 145 & 137 & 140 & 136 & 145 \\ 142 & 141 & 143 & 142 & 142 & 142 & 137 & 141 \\ 143 & 143 & 142 & 143 & 143 & 146 & 147 & 142 \\ 131 & 145 & 143 & 141 & 143 & 143 & 140 & 140 \\ 133 & 145 & 144 & 142 & 147 & 146 & 130 & 129 \\ 139 & 140 & 146 & 143 & 145 & 149 & 144 & 137 \end{bmatrix}, \quad S = \begin{bmatrix} 158 & 151 & 152 & 150 & 147 & 143 & 142 & 140 \\ 154 & 255 & 153 & 145 & 141 & 255 & 255 & 143 \\ 150 & 142 & 149 & 146 & 138 & 141 & 137 & 146 \\ 143 & 142 & 144 & 143 & 143 & 143 & 138 & 142 \\ 142 & 142 & 141 & 142 & 142 & 145 & 146 & 141 \\ 130 & 144 & 255 & 140 & 142 & 142 & 139 & 139 \\ 132 & 144 & 255 & 141 & 146 & 145 & 129 & 128 \\ 138 & 139 & 255 & 142 & 144 & 148 & 143 & 255 \end{bmatrix}, \quad (1)$$

тоді як вбудовування біта ДІ $d = 1$ у стеганоповідомлення відбулося із застосуванням кодового слова $T^{+}_{16,(5,1)}$, що вибірково впливає на трансформанту перетворення Уолша-Адамара (5,1). Знайдемо матрицю Δ різниці між матрицями блоків стеганоповідомлення і оригінального повідомлення

$$\Delta = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 111 & 1 & 1 & 1 & 112 & 114 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 112 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 111 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 109 & -1 & -1 & -1 & -1 & 118 \end{bmatrix}. \quad (2)$$

Ми бачимо, що після поелеметного множення елементів отриманої матриці Δ на елементи застосованого кодового слова $T^{+}_{16,(5,1)}$, із подальшим підсумовуванням елементів результуючої матриці, і застосуванням операції $sign()$ отримуємо значення біта ДІ $d' = sign(\sum_{i=1}^{8}\sum_{j=1}^{8}\Delta(i,j)\circ T^{+}_{16,(5,1)}(i,j)) = sign(-56) = -1$, що не відповідає вбудованому біту ДІ, тобто приводить до помилки при вилученні ДІ.

Здійснимо обмеження амплітуди відповідно до методу ШОВ, в результаті чого отримуємо матрицю різниці

$$\Delta = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ -1 & -1 & -1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & -1 & -1 & -1 & -1 & -1 \\ -1 & -1 & 1 & -1 & -1 & -1 & -1 & 1 \end{bmatrix}, \quad (3)$$

для якої після поелеметного множення елементів отриманої матриці Δ на елементи кодового слова $T^{+}_{16,(5,1)}$ із подальшим підсумовуванням елементів результуючої матриці і застосуванням операції $sign()$, отримуємо значення біта ДІ $d' = sign(\sum_{i=1}^{8}\sum_{j=1}^{8}\Delta(i,j)\circ T^{+}_{16,(5,1)}(i,j)) = sign(56) = 1$, що відповідає вбудованому біту ДІ.

Задля оцінки рівня підвищення стійкості стеганографічного методу з кодовим управлінням вбудовуванням ДІ до атаки зашумленням шумом «Salt and Pepper» був проведений обчислювальний експеримент із застосуванням 500 зображень з бази NRCS [10], що був спрямований на оцінку кількості помилок при вилученні ДІ з стеганоповідомлення в умовах атаки зашумленням, рівень якого вимірювався показником PSNR. При цьому для вбудовування ДІ застосовувалося кодове слово $T^{+}_{b,8,(5,1)}$, що впливає на трансформанту перетворення Уолша-Адамара (5,1) без застосування ШОВ, а також те саме кодове слово із застосуванням ШОВ (BAN $T^{+}_{b,8,(5,1)}$). Результати проведеного експерименту продемонстровані на рис. 2.

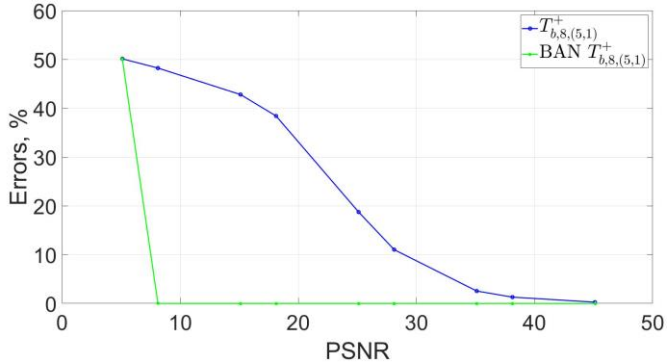

Рис 2. Залежність числа помилок при вилученні ДІ від інтенсивності шуму «Salt and Pepper»

Таким чином, підвищення стійкості стеганографічного методу з кодовим управлінням вбудовуванням ДІ до атак зашумленням шумом «Salt and Pepper» має місце на рівні до 48% (рис. 2) для випадку кодового слова $T^{+}_{b,8,(5,1)}$ порядку $\mu = 8$, що впливає на трансформанту Уолша-Адамара (5,1).Застосування обмеження амплітуди перед обробкою матриць різниць є важливим кроком для забезпечення якості відновлення ДІ. Воно допомагає уникнути впливу шумових компонентів, що можуть спотворити ДІ. Таким чином, обмеження амплітуди допомагає підвищити надійність та стійкість стеганографічного методу з кодовим управлінням вбудовуванням ДІ до атак зашумленням.

Висновки. У даній роботі було проведено дослідження, що мало на меті підвищення стійкості стеганографічного методу з кодовим управлінням вбудовуванням ДІ в умовах атак зашумленням шумом АБГШ та шумом «Salt and Pepper».

Показано, що у випадку атаки проти вбудованого повідомлення зашумленням АБГШ стійкість стеганографічного методу є інваріантною до структури застосовуваного кодового слова. Стійкість методу може бути підвищеною за рахунок збільшення енергії кодового слова, що можливо із застосуванням багаторівневих кодових слів, при чому раціональним є застосуванням багаторівневих кодових слів, що здійснюють вибірковий вплив на високі частоти задля підвищення надійності сприйняття стеганоповідомлення і уникнення проблеми виникнення областей із перепадами яскравості на границях блоків.

В каналах з шумом типу «Salt and Pepper» було запропоновано застосування методу ШОВ, що передбачає обмеження по амплітуді матриць різниці стеганоповідомлення та оригінального контейнеру. Застосування даного методу дозволило знизити рівень помилок на 48% у порівняння із застосуванням оригінального стеганографічного методу з кодовим управлінням вбудовуванням ДІ.

Рекомендації, запропоновані у роботі, можуть бути використані для подальшого вдосконалення та оптимізації методу.

Список літератури

1. Мельник М.А. Стеганоалгоритм, устойчивый к сжатию. *Інформаційна безпека*. 2012. №2(8). С. 99-106.
2. Song X. et al. Robust JPEG steganography based on DCT and SVD in nonsubsampled shearlet transform domain. *Multimedia Tools and Applications*. 2022. Vol. 81. No. 25. P. 36453-36472.
3. Durafe A., Patidar V. Development and analysis of IWT-SVD and DWT-SVD steganography using fractal cover. *Journal of King Saud University-Computer and Information Sciences*. 2022. Vol. 34. No. 7. P. 4483-4498.
4. Arunkumar S. et al. SVD-based robust image steganographic scheme using RIWT and DCT for secure transmission of medical images. *Measurement*. 2019. Vol. 139. P. 426-437.
5. Pilania U., Tanwar R., Gupta P. An ROI-based robust video steganography technique using SVD in wavelet domain. *Open Computer Science*. 2022. Vol. 12. No. 1. P. 1-16.
6. Hussain M. et al. Image steganography in spatial domain: A survey. *Signal Processing: Image Communication.* 2018. Vol. 65. P. 46-66.
7. Rachael O. et al. Image steganography and steganalysis based on least significant bit (LSB). Proceedings of ICETIT 2019: Emerging Trends in Information Technology. Delhi, India: Springer International Publishing, 2020. P. 1100-1111.

8. Msallam M. M. A development of least significant bit steganography technique. *Iraqi journal of computers, communications, control and systems engineering*. 2020. Vol. 20. No. 1. P. 31-39.
9. Kobozeva A.A., Sokolov A.V. Robust Steganographic Method with Code-Controlled Information Embedding. *Problemele energeticii regionale*. 2021. No. 4 (52). P. 115-130.
10. NRCS Photo Gallery // United States Department of Agriculture. URL: https://www.nrcs.usda.gov/wps/portal/nrcs/main/national/newsroom/multimedia/
11. Грибунин В.Г., Оков И.Н., Туринцев И.В. Цифровая стеганография. М.: Солон-Пресс, 2002. 272 с.
12. Kobozeva A.A., Sokolov A.V. Theoretical foundations for constructing effective codewords for the code-controlled information embedding steganographic method. *Radiotekhnika*. 2021. 4(207). P. 27-39.

INCREASING THE ROBUSTNESS OF THE STEGANOGRAPHIC METHOD WITH CODE CONTROL OF THE ADDITIONAL INFORMATION EMBEDDING AGAINST NOISE ATTACKS

D.O. Hulid, A.V. Sokolov

National Odesa Polytechnic University
Ukraine, Odesa, 65044, Shevchenko Ave., 1, radiosquid@gmail.com

The increase in the amount of multimedia content generated, stored and transmitted by modern information systems leads to an increase in the role of the steganographic component in information protection systems. At the same time, significant requirements are put to the applied steganographic methods regarding their effectiveness, which include sufficient bandwidth, ensuring the reliability of perception, and resistance to attacks against the embedded message. The performance of the steganographic methods is of great importance, especially if it is intended to be used in real-time on a resource-constrained platforms. One of the modern steganographic methods, which is characterized by providing the main effectiveness indicators with a small computational complexity due to the execution of steganographic transformation in the space domain of the container, is a steganographic method with code control of additional information embedding. However, despite the rather high indicators of resistance to noise attacks, which can occur in many practical applications, the issue of increasing the resistance of steganographic transformation to these types of attacks remains relevant. The purpose of the paper is to increase the resistance to noise attacks of the steganographic method with code control of additional information embedding. The paper researches attacks against an embedded message with two types of noise: additive white Gaussian noise and “Salt and Pepper” noise. In the paper, experimental research on the effects of the structure of the codeword used on the robustness of the steganographic method with code control against a noise attack by additive white Gaussian noise was performed, which made it possible to develop practical recommendations regarding the parameters of the steganographic method with code control under the conditions of this type of attack. The application of the BAN method (broadband signal, attenuator, narrowband signal) is proposed to increase the resistance of the steganographic method with code control against the "Salt and Pepper" noise attack, which allowed to reduce the number of errors when extracting additional information in conditions of this noise by 48%. The results obtained in this paper can be useful for the application of the steganographic method with code control in practice in the conditions of transmission of a steganographic message over channels characterized by the presence of noise attacks against the embedded message.
Keywords: steganography, code control of additional information embedding, noise attack, additive white Gaussian noise, “Salt and Pepper” noise.