Магістерська кваліфікаційна робота на тему:

«Підвищення стійкості методу забезпечення автентичності цифрових зображень доказової бази судової системи від несанкціонованих модифікацій»

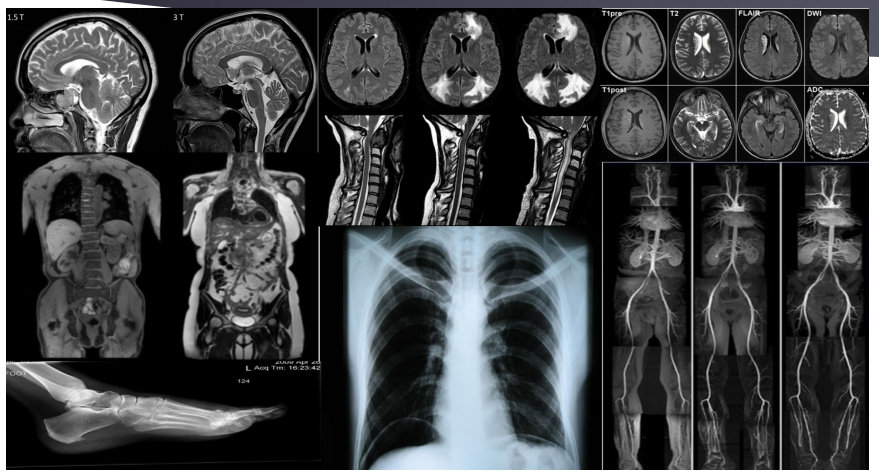
СТУДЕНТА ГРУПИ УБ-17М *Павленка Б.В.*

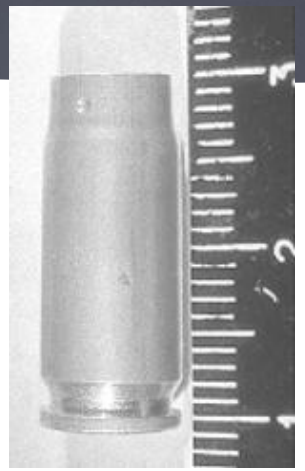
КЕРІВНИК: К.Т.Н., ДОЦ. КАРПІНЕЦЬ В.В.

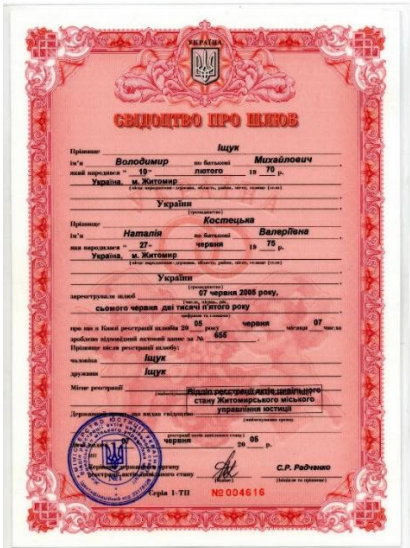
Мета, об'єкт, предмет:

- Метою дипломної роботи є вдосконалення методу забезпечення автентичності цифрових зображень для використання в судовій системі зі збільшенням стійкості методу до несанкціонованих модифікацій.
- Об'єкт дослідження роботи – процес забезпечення автентичності цифрових растрових зображень.
- Предмет дослідження – існуючі методи та засоби забезпечення автентичності цифрових зображень.

Види зображень доказової бази судової системи







Метод забезпечення автентичності зображень судової системи

- Використання алгоритму Коха-Жао для вбудовування ЦВЗ
- Використання алгоритму SHA-512 (SHA-2) для генерації значення хеш-функції
- Збереження даних про операцію

Стеганографічний метод Коха-Жао

- Розбиття зображення на блоки 8 х 8
- Застосування до кожного блоку ДКП

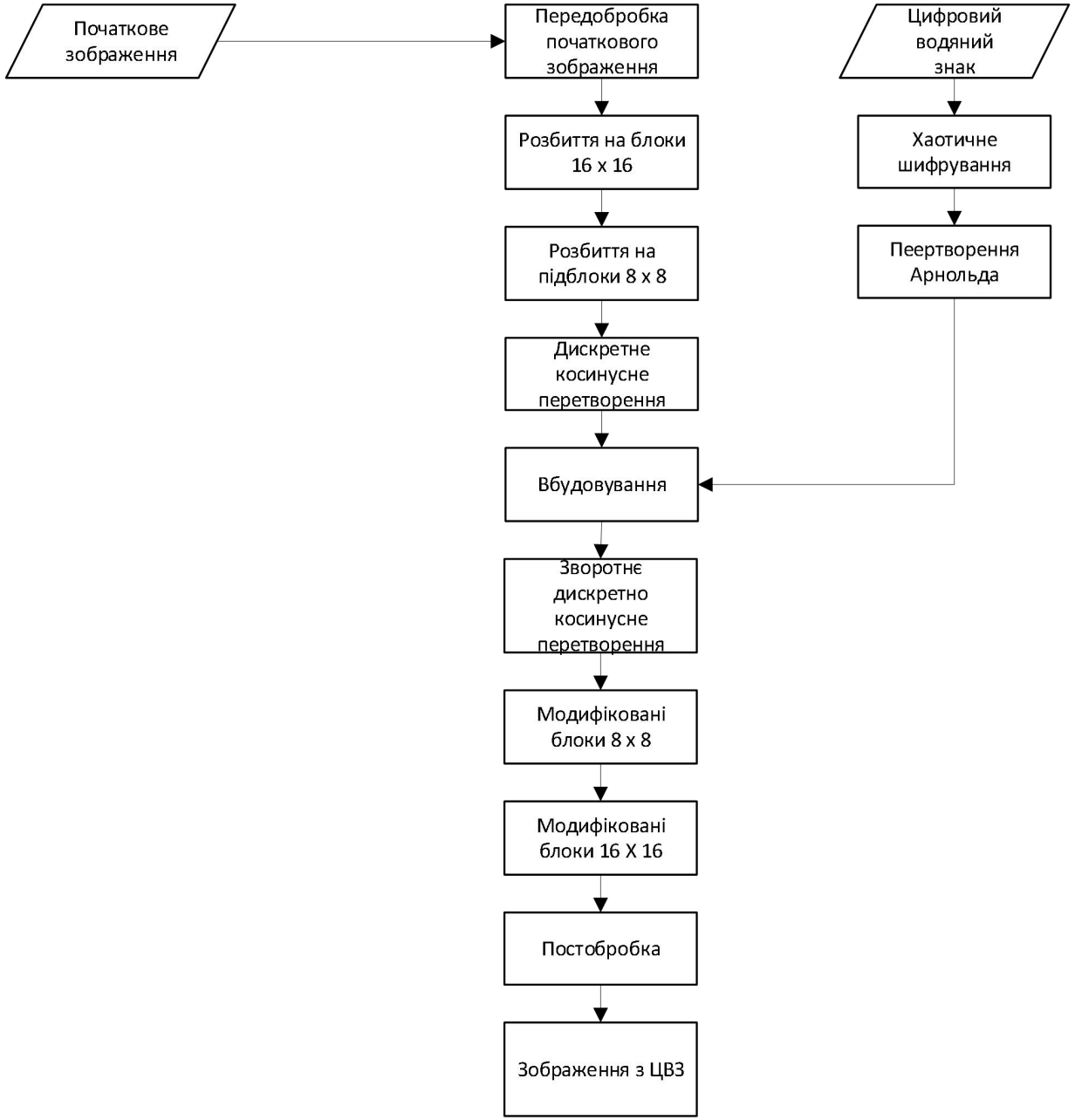
$$\sigma(\upsilon,\nu)=\frac{\zeta(\upsilon)\cdot\zeta(\nu)}{\sqrt{2N}}\cdot\sum_{x=0}^{N-1}\sum_{y=0}^{N-1}C(x,y)\cdot cos\left[\frac{\pi\cdot\upsilon\cdot(2x+1)}{2N}\right]\cdot cos\left[\frac{\pi\cdot\nu\cdot(2y+1)}{2N}\right]$$

- Отримання матриці ДКП
- Обрання випадкового блоку для початку вбудовування, вбудовування біту повідомлення
- Обрання двох симетричних відносно основної діагоналі коефіцієнтів ДКП
- Модифікація коефіцієнтів за правилом

$$\begin{cases} |\sigma_b(\upsilon_1,\nu_1)|-|\sigma_b(\upsilon_2,\nu_2)|>P, \text{при } m_b=0 \\ |\sigma_b(\upsilon_1,\nu_1)|-|\sigma_b(\upsilon_2,\nu_2)|<-P, \text{при } m_b=1 \end{cases}$$

- Виконання зворотного ДКП

Вдосконалення методу Коха-Жао



Вдосконалення методу Коха-Жао

- Попередня обробка зображення (зміна кольорової моделі, розбиття на блоки)
- Хаотичне шифрування ЦВЗ

Логічний параметр	$\mu = 1.35 + \frac{decimal(K_1)}{100}$
Значення ініціалізації алгоритму	$C_0 = 0.1 + \frac{decimal(K_2)}{17}$
Наступний елемент послідовності	$C_{n+1} = \mu \times C_n \times (1 - C_n)$

$$C`(x) = round(C(x) \times 10^4),$$
$$C``(x) = binary\left(C`(x)\right),$$
$$b(x) = xor\ all\ bits\ of\ C``(x)$$
$$w_{e1} = \mathrm{C}(x)\ XOR\ b(x)$$

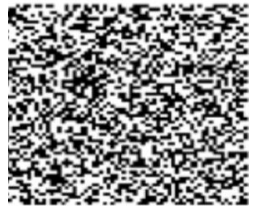
Вдосконалення методу Коха-Жао

- Виконання трансформації Арнольда

$$\begin{bmatrix} x_n \\ y_n \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \ (mod N),$$

- Зворотне перетворення Арнольда

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} 2 & -1 \\ -1 & 1 \end{bmatrix} \begin{bmatrix} x_n \\ y_n \end{bmatrix} (mod N)$$



Вдосконалення методу Коха-Жао

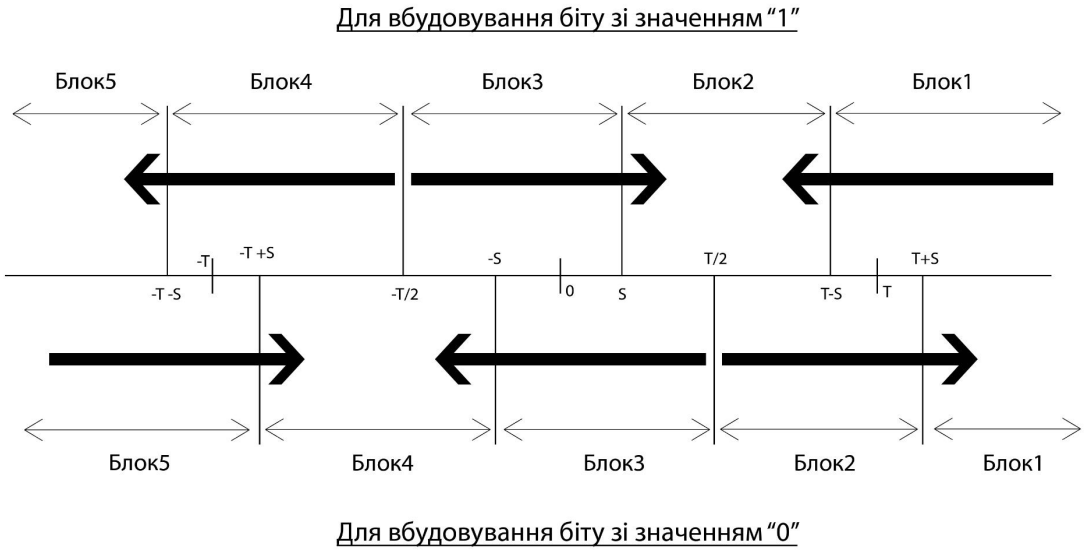


Схема алгоритму вбудовування біту ЦВЗ

$$\Delta_{xy} = \alpha \times \frac{D(C_{xy}) - Median(C_{xy})}{D(C_{xy})},$$

Фактор модифікації коефіцієнту

$$\begin{cases} |\sigma_b(\upsilon_1, \nu_1)| - |\sigma_b(\upsilon_2, \nu_2)| > P, \text{при } m_b = 0 \\ |\sigma_b(\upsilon_1, \nu_1)| - |\sigma_b(\upsilon_2, \nu_2)| < -P, \text{при } m_b = 1 \end{cases}$$

Модифікація коефіцієнтів в початковому методі

Аналіз вдосконаленого методу

$$BER = \frac{1}{mn}\left[\sum_{i=1}^{m}\sum_{j=1}^{n} w_0(i,j) \bigoplus w_x(i,j)\right]$$

$$NCC = \frac{\sum_{i=1}^{m}\sum_{j=1}^{n} w_0(i,j)w_x(i,j)}{\sum_{i=1}^{m}\sum_{j=1}^{n}[w_0(i,j)]^2},$$

Результати аналізу стійкості вдосконаленого методу

Зображення	PSNR (db)	BER (%)	NCC
Lena	46.31	0	1
Pepper	46.30	0.02	0.99
Plane	46.10	0	1
Baboon	42.72	0	1

Результати аналізу стійкості початкового методу

Зображення	PSNR (db)	BER (%)	NCC
Lena	45.27	0.03	0.99
Pepper	44.59	0.06	0.93
Plane	45.99	0.01	0.96
Baboon	41.59	0	1

Аналіз стійкості вдосконаленого методу до атак

Атака повороту зображення

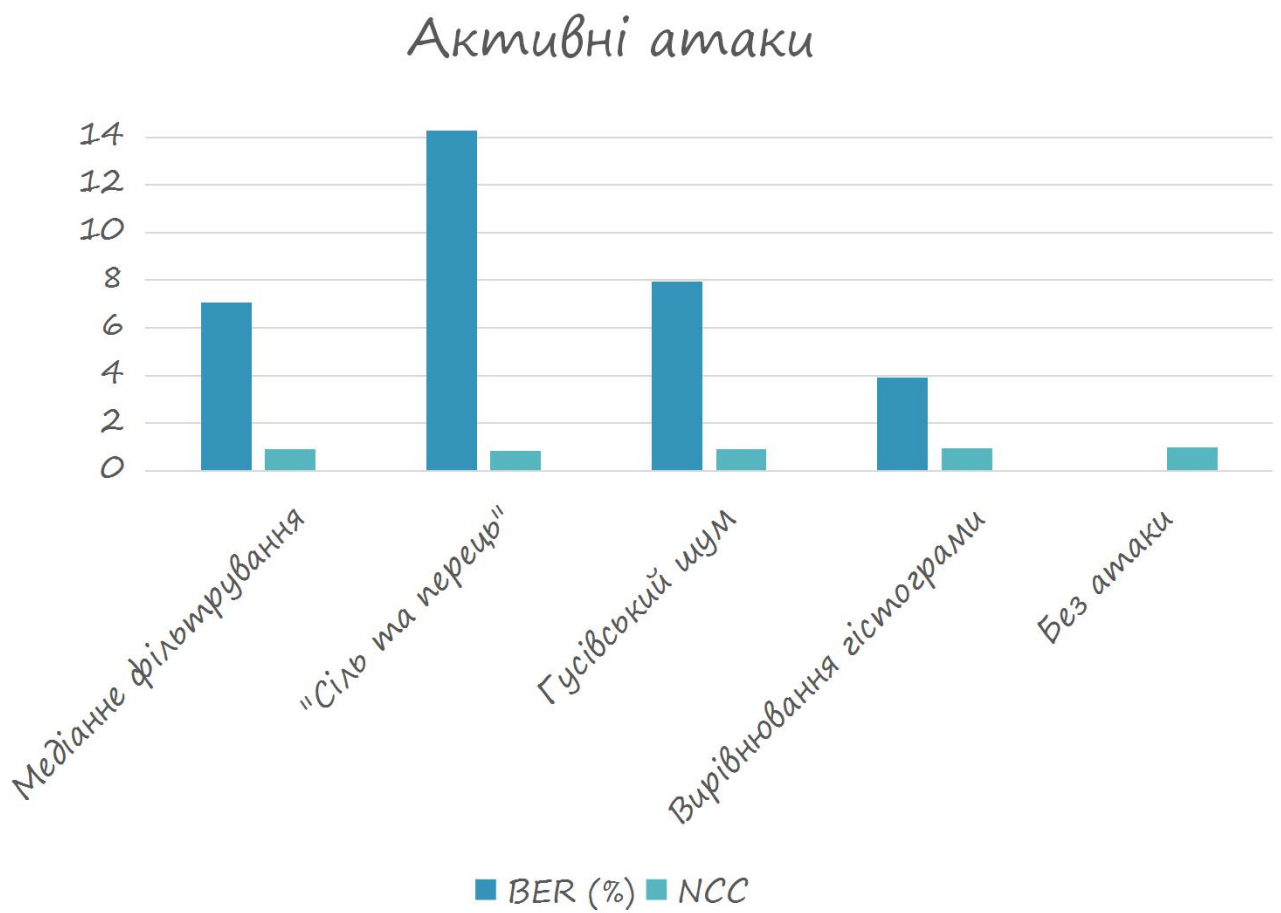
Атака відсіченням

Значення NCC для атаки відсічення

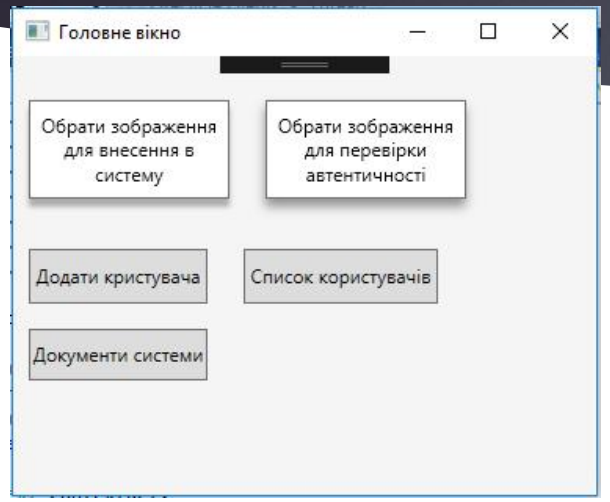
Зображення	25% лівого верхнього кута	25% правого верхнього кута	25% лівого нижнього кута	25% правого нижнього кута
Lena	0.9000	0.9027	0.9000	0.8976
Baboon	0.9007	0.9043	0.9005	0.8993
Pepper	0.8987	0.9009	0.8993	0.8994

Аналіз стійкості методу до активних атак

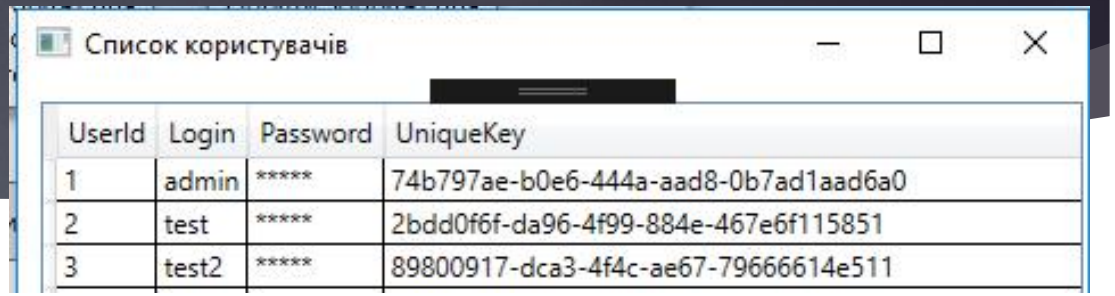
Характеристика	Медіанне фільтрування 3*3	Шум сіль та перець (0.01)	Гаусівський шум (0.001)	Вирівнювання гістограми
BER(%)	7.06	14.28	7.96	3.9
NCC	0.9258	0.8545	0.9179	0.9613



Розроблений додаток

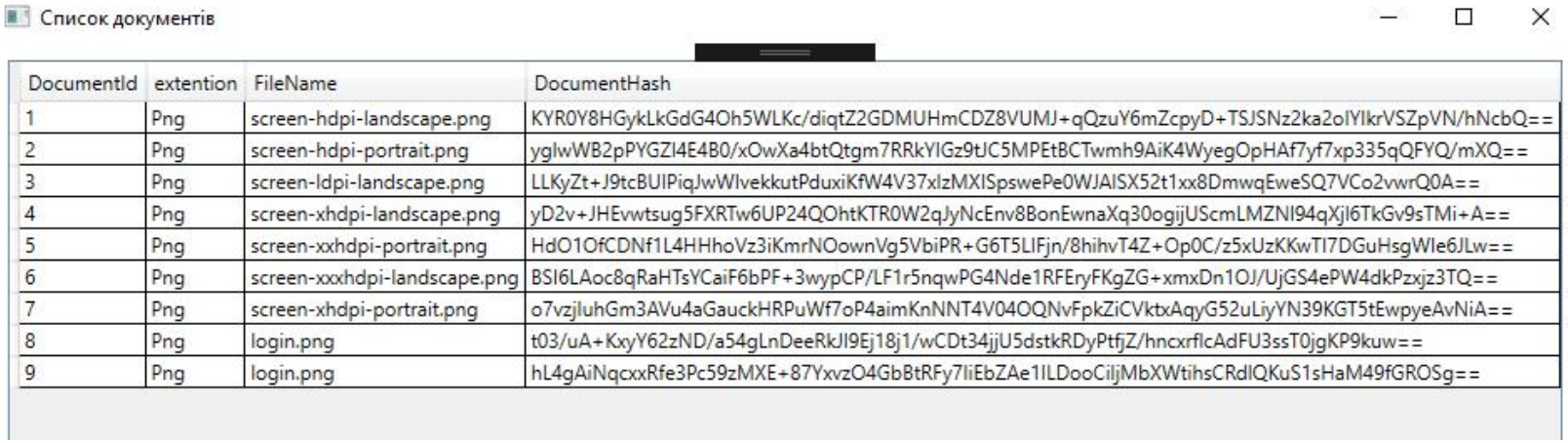


Головне вікно програми з правами адміністратора



UserId	Login	Password	UniqueKey
1	admin	*****	74b797ae-b0e6-444a-aad8-0b7ad1aad6a0
2	test	*****	2bdd0f6f-da96-4f99-884e-467e6f115851
3	test2	*****	89800917-dca3-4f4c-ae67-79666614e511

Список користувачів програми



DocumentId	extention	FileName	DocumentHash
1	Png	screen-hdpi-landscape.png	KYR0Y8HGykLkGdG4Oh5WLKc/diqtZ2GDMUHmCDZ8VUMJ+qQzuY6mZcpyD+TSJSNz2ka2olYlkrVSZpVN/hNcbQ==
2	Png	screen-hdpi-portrait.png	yglwWB2pPYGZl4E4B0/xOwXa4btQtgm7RRkYlGz9tJC5MPEtBCTwmh9AiK4WyegOpHAf7yf7xp335qQFYQ/mXQ==
3	Png	screen-ldpi-landscape.png	LLKyZt+J9tcBUIPiqJwWlvekkutPduxiKfW4V37xlzMXISpswePe0WJAISX52t1xx8DmwqEweSQ7VCo2vwrQ0A==
4	Png	screen-xhdpi-landscape.png	yD2v+JHEvwtsug5FXRTw6UP24QOhtKTR0W2qJyNcEnv8BonEwnaXq30ogijUScmLMZNI94qXjl6TkGv9sTMi+A==
5	Png	screen-xxhdpi-portrait.png	HdO1OfCDNf1L4HHhoVz3iKmrNOownVg5VbiPR+G6T5LIFjn/8hihvT4Z+Op0C/z5xUzKKwTI7DGuHsgWIe6JLw==
6	Png	screen-xxxhdpi-landscape.png	BSI6LAoc8qRaHTsYCaiF6bPF+3wypCP/LF1r5nqwPG4Nde1RFEryFKgZG+xmxDn1OJ/UjGS4ePW4dkPzxjz3TQ==
7	Png	screen-xhdpi-portrait.png	o7vzjluhGm3AVu4aGauckHRPuWf7oP4aimKnNNT4V04OQNvFpkZiCVktxAqyG52uLiyYN39KGT5tEwpyeAvNiA==
8	Png	login.png	t03/uA+KxyY62zND/a54gLnDeeRkJI9Ej18j1/wCDt34jjU5dstkRDyPtfjZ/hncxrflcAdFU3ssT0jgKP9kuw==
9	Png	login.png	hL4gAiNqcxxRfe3Pc59zMXE+87YxvzO4GbBtRFy7liEbZAe1ILDooCiljMbXWtihsCRdlQKuS1sHaM49fGROSg==

Список документів внесених до системи

Висновки

- Вдосконалено метод забезпечення автентичності цифрових зображень доказової бази судової системи для підвищення стійкості від несанкціонованих модифікацій.
- Досліджено можливості вдосконалення методу.
- Вдосконалено стеганографічний алгоритм Коха-Жао за рахунок використання хаотичного шифрування, трансформації Арнольда та модифікації алгоритму вбудовування бітів ЦВЗ.
- Розроблено програмне забезпечення для реалізації вдосконаленого методу.
- Проаналізовано стійкість розробленого методу до атак.
- Розраховано економічну цінність розробки та доведено її доцільність.

Дякую за увагу!