УДК 003.26:004.057.4

Неласа Г. В.[1], Дозоренко І. С.[2]

[1]Доцент Запорізького національного технічного університету
[2]Магістрант Запорізького національного технічного університету

ОГЛЯД ТА ПОРІВНЯННЯ СХЕМ ЦИФРОВИХ МУЛЬТИПІДПИСІВ

Розглянуто декілька відомих схем цифрових мультипідписів із груповою перевіркою чинності, які використовують лише одну замість кількох перевірок, та недоліки цих схем. Властивості схем порівняно за кількома критеріями.

Ключові слова: цифровий підпис, мультипідпис, групова перевірка, RSA, DSA.

ВСТУП

Цифровий підпис – це назва схожого на традиційний підпис методу, що використовується в криптографії. При використанні традиційного підпису людина пише своє власне ім'я на папері. Ніхто не може підробити інший підпис, тому що важко імітувати чужий почерк. Для впровадження цифрового підпису використовують криптосистеми з відкритим ключем. Кожний підпис має пару ключів: секретний ключ і відкритий ключ. Секретний ключ зберігається у таємниці, у той час як відкритий ключ оприлюднений. Відправник може підписати електронний документ за допомогою цифрового підпису з використанням свого секретного ключа, а одержувач може перевірити цифровий підпис з використанням відкритого ключа відправника. Ніхто не може підробити чужий цифровий підпис, тому що закритий ключ зберігається у таємниці.

Існує багато модифікацій стандартної схеми цифрового підпису, одна з яких, мультипідпис, дозволяє зменшити час верифікації для багатьох підписів. Метою даної роботи є огляд схем цифрових мультипідписів із груповою перевіркою чинності та порівняння їх властивостей.

1. ПОСТАНОВКА ЗАДАЧІ

Традиційно, якщо Аліса хоче відправити повідомлення m, де $m \ p$, Бобу, m повинні бути розділені на t копій $m_1, m_2, \ldots, m_t$. Тоді Аліса підписує ці повідомлення t разів для створення кількох цифрових підписів і відсилає ці повідомлення із цифровими підписами до Боба. Після отримання Боб повинен t разів провести перевірку чинності цих цифрових підписів. Як можна бачити, це потребує багатьох обчислень ступеня за модулем. У випадку використання хеш-функції довжина повідомлення не має значення, але перевірка може займати багато часу через велику кількість повідомлень, що були відправлені.

Для вирішення цієї проблеми Naccache та ін. у 1994 році запропонували схему цифрового мультипідпису із груповою перевіркою [1]. Верифікатор може перевірити цей цифровий мультипідпис за допомогою відкритого ключа, при цьому потрібна тільки одна замість кількох перевірок. Однак, Lim і Lee зазначили [2], що в цій схемі цифровий мультипідпис може бути легко підроблений, для того щоб пройти групову перевірку чинності. У 1998 році Harn запропонував два методи групової перевірки чинності цифрового мультипідпису [3, 4]. Разом з тим, Hwang та ін. зазначили, що ці схеми також не є безпечними [5, 6]. Зловмисник може підробити цифровий мультипідпис для того, щоб пройти групову перевірку чинності. Тому вони запропонували два удосконалення [7]. У 2001 році Shao також запропонував поліпшення для схеми Harn'а [8].

Можна побачити, що якщо цифровий мультипідпис підроблений зловмисником, то має бути перевірений кожний з цифрових підписів. Це означає повернення до вихідної схеми цифрового підпису, яка потребує t перевірок. У 2002 році Changchien і Hwang запропонували алгоритм ефективного виявлення підроблених цифрових мультипідписів [9].

2. СХЕМА NACCACHE ТА ЇЇ НЕДОЛІКИ

Схема мультипідпису Naccache отримана за допомогою модифікації схеми DSA, в якій рівняння перевірки підпису має такий вигляд:

$$r = (g^{ms^{-1}} y^{rs^{-1}} \bmod p) \bmod q, \qquad (1)$$

де $r = g^k \bmod p$, $s = k^{-1}(m + xr) \bmod q$; m – повідомлення; $y = g^x \bmod p$ – відкритий ключ особи, що підписує документ; x – секретний ключ особи, що підписує документ; p – велике просте число; q – великий простий дільник $p - 1$; g – елемент з Z_p порядку q.

Для прискорення перевірки кількох цифрових підписів Naccache та ін. у 1994 році запропонували схему для групової перевірки цифрового мультипідпису. Верифікатор може перевіряти кілька цифрових підписів із використанням відкритого ключа відправника, якому потрібна тільки одна замість t перевірок. Схема виглядає таким чином:

1) Припустимо, що Аліса хоче відправити Бобу t повідомлень $(m_1, m_2, \ldots, m_t)$ та цифровий мультипідпис (r_1, s_1), (r_2, s_2), …, (r_t, s_t). Цифровий мультипідпис був створений за алгоритмом цифрового підпису DSA.

2) Після отримання t повідомлень $(m_1, m_2, \ldots, m_t)$ та мультипідпису (r_1, s_1), (r_2, s_2), …, (r_t, s_t) Боб може перевірити чинність мультипідпису для повідомлень $(m_1, m_2, \ldots, m_t)$ з використанням відкритого ключа Аліси за допомогою рівняння

$$\prod_{i=1}^{t} r_i \bmod p \equiv g^{\sum_{i=1}^{t} -m_i s_i^{-1} \bmod q} \; y^{\sum_{i=1}^{t} r_i s_i^{-1} \bmod q} \bmod p. \quad (2)$$

3) Якщо рівняння виконується, то Боб може стверджувати, що цифровий мультипідпис (r_1, s_1), (r_2, s_2), …, (r_t, s_t) був створений Алісою.

Очевидно, що Боб може зробити групову перевірку цифрового мультипідпису, для чого потрібне тільки одне рівняння (2). Таким чином, схема Naccache та ін. є більш доцільною для групової перевірки кількох цифрових підписів.

Однак Lim і Lee показали, що схема Naccache не є безпечною. Вона має вразливість, завдяки якій зловмисник може підробити цифровий мультипідпис так, щоб рівняння групової перевірки 1.2 виконувалось. Нижче описано спосіб атаки.

1) Зловмисник вибирає довільні числа (u_i, v_i), $i = 1, 2, \ldots, t$ і обчислює $r_i = g^{u_i} y^{v_i} \bmod p$, $i = 1, 2, \ldots, t$.

2) Обчислює $s_b^{-1} \bmod q$, що задовольняє $v_b = r_b s_b^{-1} \bmod q$, $b = 1, 2, \ldots, t$.

3) Зловмисник може отримати s_{t-1} та s_t з рівнянь:

$$\sum_{i=1}^{t} u_i = \sum_{i=1}^{t} m_i s_i^{-1} \bmod q,$$

$$\sum_{i=1}^{t} v_i = \sum_{i=1}^{t} r_i s_i^{-1}.$$

Звідси видно, що зловмисник може підробити t повідомлень $m_1, m_2, \ldots, m_t$ та цифровий мультипідпис (r_1, s_1), (r_2, s_2), …, (r_t, s_t) для того, щоб рівняння групової перевірки (2) виконувалось. Однак жоден з цих підроблених підписів окремо не проходить перевірку в рівнянні (1).

3. СХЕМА ЦИФРОВОГО RSA МУЛЬТИПІДПИСУ HARN'A ТА ЇЇ НЕДОЛІКИ

Схема мультипідпису заснована на алгоритмі RSA, в якій рівняння перевірки підпису має такий вигляд:

$$h(m_i) = S_i^e \bmod n, \quad (3)$$

де $n = p \times q$; $e \times d \bmod (p-1)(q-1) \equiv 1$; p, q – великі прості числа.

Тепер припустимо, що Аліса бажає відправити Бобу t повідомлень $(m_1, m_2, \ldots, m_t)$ та цифровий мультипідпис $S_1, S_2, \ldots, S_t$. Цифровий мультипідпис був створений за алгоритмом RSA, поданим вище. Отже, Аліса відсилає Бобу (m_i, S_i), $i = 1, 2, \ldots, t$.

Після отримання t повідомлень $(m_1, m_2, \ldots, m_t)$ та мультипідпису $S_1, S_2, \ldots, S_t$ Боб може перевірити чинність мультипідпису для повідомлень $(m_1, m_2, \ldots, m_t)$ із використанням відкритого ключа Аліси e за допомогою рівняння

$$\left(\prod_{i=1}^{t} S_i \right)^e = \prod_{i=1}^{t} h(m_i) \bmod n. \quad (4)$$

Якщо рівняння виконується, то Боб може стверджувати, що цифровий мультипідпис $S_1, S_2, \ldots, S_t$ належить Алісі. Очевидно, що Боб може зробити групову перевірку цифрового мультипідпису, для чого потрібне тільки одне рівняння (4). Таким чином, схема Harn'a є більш доцільною для групової перевірки кількох цифрових підписів.

Hwang та ін. запропонували дві атаки для схеми Harn'a. Вони довели, що особа, яка підписує документ, може підробити цифровий мультипідпис так, щоб рівняння групової перевірки (4) виконувалось. Після цього особа може заперечувати, що саме вона підписала ці документи, тобто не виконується умова про неможливість відмови від авторства. Нижче описані способи атаки.

Перший спосіб атаки. Аліса відсилає Бобу підроблені сукупності (m_i, S_i'), $i = 1, 2, \ldots, t$, де $S_i' = h(m_{f(i)})^d \bmod n$, $i = 1, 2, \ldots, t$; $f(\,)$ – бієкція, для якої $f(i) = j$, $i = 1, 2, \ldots, t$ та $j = 1, 2, \ldots, t$. Якщо після отримання підроблених сукупностей (m_i, S_i') Боб перевірить чинність мультипідпису для повідомлень із використанням рівняння групової перевірки (4), то він може стверджувати, що цифровий мультипідпис $S_1', S_2', \ldots, S_t'$ належить Алісі.

Другий спосіб атаки. Аліса відсилає Бобу підроблені сукупності (m_i, S_i'), $i = 1, 2, \ldots, t$, де $S_i' = a_i \times S_i \bmod n$, $i = 1, 2, \ldots, t$ та $\prod_{i=1}^{t} a_i = 1$. Якщо

після отримання підроблених сукупностей (m_i, S_i') Боб перевірить чинність мультипідпису для повідомлень із використанням рівняння групової перевірки (4), то він може стверджувати, що цифровий мультипідпис S_1', S_2', …, S_t' належить Алісі.

Встановлено, що жоден з цих підроблених підписів окремо не проходить RSA перевірку з використанням рівняння (3). Таким чином, Аліса може заперечувати, що вона підписала документи. Схема не відповідає умові про неможливість відмови від авторства.

4. СХЕМА ЦИФРОВОГО DSA-TYPE МУЛЬТИПІДПИСУ HARN'A ТА ЇЇ НЕДОЛІКИ

Схема мультипідпису заснована на алгоритмі DSA-type, що є подібним до алгоритму DSA. Рівняння верифікації має такий вигляд:

$$r = (g^{sr^{-1}} y^{mr^{-1}} \bmod p) \bmod q, \qquad (5)$$

де $r = (g^k \bmod p) \bmod q$; $s = rk - mx \bmod q$; m – повідомлення; $y = g^x \bmod p$ – відкритий ключ особи, що підписує документ; x – секретний ключ особи, що підписує документ; p – велике просте число; q – великий простий дільник $p - 1$; g – елемент з Z_p порядку q.

Для прискорення перевірки кількох цифрових підписів Harn запропонував схему для групової перевірки цифрових підписів. Схема виглядає таким чином:

1) Припустимо, що Аліса хоче відправити Бобу t повідомлень $(m_1, m_2, \ldots, m_t)$ та цифровий мультипідпис (r_1, s_1), (r_2, s_2), …, (r_t, s_t). Цифровий мультипідпис був створений за алгоритмом цифрового підпису DSA-type.

2) Після отримання t повідомлень $(m_1, m_2, \ldots, m_t)$ та мультипідпису (r_1, s_1), (r_2, s_2), …, (r_t, s_t) Боб може перевірити чинність мультипідпису для повідомлень $(m_1, m_2, \ldots, m_t)$ із використанням відкритого ключа Аліси за допомогою рівняння

$$\prod_{i=1}^{t} r_i = \left(g^{\sum_{i=1}^{t} s_i r_i^{-1}} y^{\sum_{i=1}^{t} m_i r_i^{-1}} \bmod p \right) \bmod q. \qquad (6)$$

3) Якщо рівняння виконується, то Боб може стверджувати, що цифровий мультипідпис (r_1, s_1), (r_2, s_2), …, (r_t, s_t) був створений Алісою.

Очевидно, що Боб може зробити групову перевірку цифрового мультипідпису, для чого потрібне тільки одне рівняння (6). Таким чином, схема Harn'a є більш доцільною для групової перевірки кількох цифрових підписів.

Hwang та ін. показали, що схема Harn'a не є безпечною. Вона має вразливість, завдяки якій особа, що підписує документ, може підробити цифровий мультипідпис так, щоб рівняння групової перевірки (6) виконувалось. Після цього особа може заперечувати, що саме вона підписала ці документи, тобто не виконується умова про неможливість відмови від авторства. Нижче описано спосіб атаки.

1) Аліса відсилає Бобу підроблені сукупності (m_i, r_i, s_i'), $i = 1, 2, \ldots, t$, де $s_i' = s_i + a_i r_i \bmod q$, і a_i – ціле число, для якого $\sum_{i=1}^{t} a_i = 0$.

2) Якщо після отримання підроблених сукупностей (m_i, r_i, s_i') Боб перевірить чинність мультипідпису для повідомлень із використанням рівняння групової перевірки (6), то він може стверджувати, що цифровий мультипідпис (r_1, s_i'), (r_2, s_2'), (r_2, s_i') був створений Алісою.

Встановлено, що жоден з цих підроблених підписів окремо не проходить DSA-type перевірку з використанням рівняння (5). Таким чином, Аліса може заперечувати, що вона підписала документи. Схема не відповідає умові про неможливість відмови від авторства, тому що $r \neq (g^{s_i' r_i^{-1}} y^{m_i r_i^{-1}} \bmod p) \bmod q$, $i = 1, 2, \ldots, t$.

5. СХЕМИ ЦИФРОВОГО МУЛЬТИПІДПИСУ HWANG'A

Щоб виправити слабкі сторони схеми цифрового RSA-type мультипідпису Harn'a і схеми цифрового DSA мультипідпису Harn'a, Hwang та ін. запропонували два вдосконалення для цих схем. Перше є поліпшенням схеми цифрового RSA мультипідпису (скорочено BV-RSA). Різниця полягає в рівнянні (3):

$$\left(\prod_{i=1}^{t} S_i^{v_i} \right)^{e} = \prod_{i=1}^{t} h(m_i^{v_i}) \bmod n, \qquad (7)$$

де v_i, $i = 1, 2, \ldots, t$ є невеликими довільними числами, що обираються перевіряючим.

Друге є поліпшенням схеми цифрового DSA-type мультипідпису (скорочено BV-DSA). Єдина різниця полягає в рівнянні (6). Його модифіковано таким чином:

$$\prod_{i=1}^{t} r_i^{v_i} = \left(g^{\sum_{i=1}^{t} s_i r_i^{-1} v_i} y^{\sum_{i=1}^{t} m_i r_i^{-1} v_i} \bmod p \right) \bmod q, \qquad (8)$$

де v_i, $i = 1, 2, \ldots, t$, є невеликими довільними числами, що обираються перевіряючим.

6. СХЕМА ЦИФРОВОГО DSA-TYPE МУЛЬТИПІДПИСУ SHAO

У 2001 році Shao запропонував схему цифрового DSA-type мультипідпису. Вона схожа на схему Hwang'a та ін. Єдина різниця полягає в рівнянні 6. Рівняння групової перевірки виглядає таким чином:

$$\prod_{i=1}^{t}(e_i(s_i))^{u_i} = \prod_{i=1}^{t}(f_i(s_i))^{u_i} \bmod p, \qquad (9)$$

де $u_i \in (1, 2^{32})$, $i = 1, 2, \ldots, t$ є довільними числами, що обираються перевіряючим, а s_i – цифровий мультипідпис, кожен підпис якого окремо задовольняє рівнянню $e_i(s_i) = f_i(s_i) \bmod p$, $i = 1, 2, \ldots, t$.

7. СХЕМА CHANGCHIEN'A ТА ІНШІ

В розділі 2 зазначено, що якщо не виконується рівняння групової перевірки, тобто $\left(\prod_{i=1}^{t} S_i\right)^e \neq \prod_{i=1}^{t} h(m_i) \bmod n$, отримувач, Боб, має перевірити кожен підпис із мультипідпису окремо з використанням рівняння $h(m_i) = S_i^e \bmod n$. Визначення підробленого підпису потребує t обчислень ступеня. У 2002 році Changchien і Hwang запропонували схему для визначення підроблених мультипідписів, що потребує лише одного обчислення ступеня та t обчислень модуля.

Changchien і Hwang перевизначили $h(\,)$ як просту необоротну хеш-функцію та $\prod_{i=1}^{t} h(m_i) \le n$. Це робить довжину $h(\,)$ рівною $\lfloor |n| / t \rfloor$ біт, де $\lfloor \cdot \rfloor$ – функція найбільшого цілого, а $|n|$ – довжина n. Для того, щоб визначити підроблений мультипідпис, Боб має виконати такі кроки:

1) Обчислити $L = \left(\prod_{i=1}^{t} S_i\right)^e \bmod n$.

2) Перевірити, чи $L \bmod h(m_i) = 0$ для $i = 1, 2, \ldots, t$.

8. ПОРІВНЯННЯ

Порівняти наведені схеми мультипідписів можна за такими критеріями:

1) *Лише чинна особа може підписати електронний документ цифровим мультипідписом.*

Всі схеми відповідають цій умові. Будь-яка особа, що має свій секретний ключ, може це зробити.

2) *Ніхто не може підробити чужий цифровий мультипідпис.*

Серед розглянутих схем лише схеми BV-DSA та BV-RSA Hwang'a, а також схема Shao відповідають цій умові. Мультипідпис за цими схемами неможливо підробити для того, щоб пройти групову перевірку чинності.

3) *Будь-який перевіряючий може провести групову перевірку чинності цифрового мультипідпису.*

Всі схеми відповідають цій умові. Будь-який перевіряючий може провести групову перевірку цього мультипідпису за допомогою відкритого ключа, для цього потрібна тільки одна перевірка.

4) *Контроль цілісності.*

Всі схеми відповідають цій умові. Зловмисник не має змоги замінити дійсний документ фальшивим, бо він не знає секретного ключа особи, що підписала документ. Лише чинна особа може підписувати свої документи.

5) *Неможливість відмови від авторства.*

Якщо відправник може підробити цифровий підпис, що проходить групову перевірку чинності, то схема не відповідає умові, бо відправник може заперечувати, що саме він відправив ці документи. Отже, лише схеми BV-DSA та BV-RSA Hwang'a, а також схема Shao відповідають цій умові.

6) *Має бути ефективний метод виявлення фальшивих цифрових мультипідписів.*

Практично всі схеми, крім схеми Changchien'a та ін., не відповідають цій умові. В цій схемі перевіряючий може ефективно визначити факт підроблення підпису.

Результати порівняння підсумовано у табл. 1, де K_i – визначені критерії, «+» – вирішено, «–» – не вирішено, ТОЗ – тип обчислювальної задачі, ЗДЛ – задача дискретного логарифмування, ЗФ – задача факторизації.

Таблиця 1. Результати порівняння схем мультипідписів

Назва схеми	K_1	K_2	K_3	K_4	K_5	K_6	ТОЗ
Naccache та ін.	+	–	+	+	–	–	ЗДЛ
DSA Harn'a	+	–	+	+	–	–	ЗДЛ
RSA Harn'a	+	–	+	+	–	–	ЗФ
BV-DSA Hwang'a	+	+	+	+	+	–	ЗДЛ
BV-RSA Hwang'a	+	+	+	+	+	–	ЗФ
Shao	+	+	+	+	+	–	ЗДЛ
Changchien'a та ін.	+	–	+	+	–	+	ЗФ

ВИСНОВКИ

Було розглянуто декілька схем цифрових мультипідписів, що вже існують. Ці схеми дозволяють будь-якому перевіряючому проводити групову перевірку чинності цифрових підписів. Вони дозволяють заощадити багато обчислень ступеня за модулем. Тим не менш, лише схеми BV-DSA та BV-RSA Hwang'a, а також схема Shao є надійними та забезпечують умову неможливості відмови від авторства. Однак ці схеми не мають ефективного методу виявлення підроблених підписів на відміну від схеми Changchien'a. Проблема створення безпечної та ефективної схеми цифрового мультипідпису залишається відкритою та може розглядатися як напрямок подальших досліджень.

СПИСОК ЛІТЕРАТУРИ

1. *Naccache, D.* Can DSA be improved: Complexity trade-os with the digital signature standard / D. Naccache, D. Mraihi, D. Rapheali, S. Vaudenay // Proceedings of Eurocrypt'94. – 1994. – Pp. 85–94.
2. *Lim, C. H.* Security of interactive DSA batch verication / C. H. Lim, P. J. Lee // Electronics Letters. – 1994. – Vol. 30, No. 19. – Pp. 1592–1593.
3. *Harn, L.* Batch verifying multiple DSA-type digital signatures // Electronics Letters. – 1998. – Vol. 34, No. 9. – Pp. 870–871.
4. *Harn, L.* Batch verifying multiple RSA digital signatures // Electronics Letters. – 1998. – Vol. 34, No. 12. – Pp. 1219–1220.
5. *Hwang, M. S.* Cryptanalysis of the batch verifying multiple RSA digital signatures / M. S. Hwang, I. C. Lin, K. F. Hwang // Informatica. – 2000. – Vol. 11, No. 1. – Pp. 15–19.
6. *Hwang, M. S.* Cryptanalysis of the batch verifying multiple DSA-type digital signatures / M. S. Hwang, C. C. Lee, Eric J. L. Lu // Pakistan Journal of Applied Sciences. – 2001. – Vol. 1, No. 3. – Pp. 287–288.
7. *Hwang, M. S.* Two simple batch verifying multiple digital signatures / M. S. Hwang, C. C. Lee, and Y. L. Tang // The Third International Conference on Information and Communication Security (ICICS2001). – Xian, China, 2001. – Pp. 13–16.
8. *Shao, Z.* Batch verifying multiple DSA-type digital signatures // Computer Networks. – 2001. – Vol. 37, No. 3–4. – Pp. 383–389.
9. *Changchien, S. W.* A batch verifying and detecting multiple RSA digital signatures / S. W. Changchien, M. S. Hwang // International Journal of Computational and Numerical Analysis and Applications. – 2002. – Vol. 2, No. 3. – Pp. 303–307.

Надійшла 29.10.2010

Неласая А. В., Дозоренко И. С.

ОБЗОР И СРАВНЕНИЕ СХЕМ ЦИФРОВЫХ МУЛЬТИПОДПИСЕЙ

Рассмотрены известные схемы цифровых мультиподписей с групповой проверкой, использующие только одну вместо нескольких проверок, а также недостатки этих схем. Проведено сравнение свойств схем по нескольким критериям.

Ключевые слова: цифровая подпись, мультиподпись, групповая проверка, RSA, DSA.

Nelasa A. V., Dozorenko I. S.

REVIEW AND COMPARISON OF MULTIPLE DIGITAL SIGNATURES

Several batch verication multiple digital signatures are reviewed in this paper. These schemes use only one verification instead of several verifications. Weakness of these schemes is also pointed out. The schemes were compared by the defined criterions.

Key words: multiple digital signatures, batch verification, RSA, DSA.

УДК 681.142.2; 622.02.658.284; 621.325

Пелешко Д. Д.[1], Кустра Н. О.[2], Шпак З. Я.[1]

[1]Канд. техн. наук, доцент Національного університету «Львівська політехніка»

[2]Канд. техн. наук, старший викладач Національного університету «Львівська політехніка»

СУМІЩЕННЯ ЗОБРАЖЕНЬ НАБОРУ НА ОСНОВІ ВИКОРИСТАННЯ ДИСПЕРСІЇ КОЛЬОРУ ЗОБРАЖЕНЬ

Розроблено швидкий метод суміщення зображень в наборі однотипних зображень на основі розв'язання задачі майже факторизації простору топології зображень з подальшим звуженням цього простору через вирішення задачі пошуку кореляційного максимуму. Задача майже факторизації формулюється через введення напівметрики стосовно дисперсії кольору елементів топології зображення.

Ключові слова: суміщення зображень, фреймове покриття, топологія зображень, дисперсія кольору, кореляційний максимум.

ВСТУП

Традиційно для реалізації процедури знаходження і суміщення зображень використовують кореляційну прив'язку цифрових зображень. Метод кореляційної прив'язки зображень має такі недоліки:

– взаємна кореляційна функція може мати досить розмитий максимум, що ускладнює його знаходження, оскільки не враховує просторову структуру порівнюваних зображень;

– комбінаторна складність – великий перебір ситуацій [1–4].